NONRESIDENT
TRAINING
COURSE

October 1997

Information Systems Technician Training Series

Module 5—Communications Center Operations

NAVEDTRA 14226

NOTICE

Any reference within this module to "Radioman" or the former "Radioman rating" should be changed to "Information Systems Technician" and the "Information Systems Technician (IT) rating". The subject matter presented relates to the occupational standards for the IT rating.

Although the words "he," "him," and "his" are used sparingly in this course to enhance communication, they are not intended to be gender driven or to affront or discriminate against anyone.

PREFACE

By enrolling in this self-study course, you have demonstrated a desire to improve yourself and the Navy. Remember, however, this self-study course is only one part of the total Navy training program. Practical experience, schools, selected reading, and your desire to succeed are also necessary to successfully round out a fully meaningful training program.

COURSE OVERVIEW: In completing this nonresident training course, you will demonstrate a knowledge of the subject matter by correctly answering questions on the following subjects: Center Operations, Voice Communications, Emission Control, and Cryptosecurity.

THE COURSE: This self-study course is organized into subject matter areas, each containing learning objectives to help you determine what you should learn along with text and illustrations to help you understand the information. The subject matter reflects day-to-day requirements and experiences of personnel in the rating or skill area. It also reflects guidance provided by Enlisted Community Managers (ECMs) and other senior personnel, technical references, instructions, etc., and either the occupational or naval standards, which are listed in the *Manual of Navy Enlisted Manpower Personnel Classifications and Occupational Standards*, NAVPERS 18068.

THE QUESTIONS: The questions that appear in this course are designed to help you understand the material in the text.

VALUE: In completing this course, you will improve your military and professional knowledge. Importantly, it can also help you study for the Navy-wide advancement in rate examination. If you are studying and discover a reference in the text to another publication for further information, look it up.

1997 Edition Prepared by
RMCS(SW/AW) Deborah Hearn and
DPC(SW) Walter Shugar, Jr.

Published by
NAVAL EDUCATION AND TRAINING
PROFESSIONAL DEVELOPMENT
AND TECHNOLOGY CENTER

NAVSUP Logistics Tracking Number
0504-LP-026-8650

Sailor's Creed

"I am a United States Sailor.

I will support and defend the Constitution of the United States of America and I will obey the orders of those appointed over me.

I represent the fighting spirit of the Navy and those who have gone before me to defend freedom and democracy around the world.

I proudly serve my country's Navy combat team with honor, courage and commitment.

I am committed to excellence and the fair treatment of all."

CONTENTS

SUMMARY OF THE RADIOMAN TRAINING SERIES

MODULE 1

Administration and Security—This module covers Radioman duties relating to administering AIS and communication systems. Procedures and guidance for handling of classified information, messages, COMSEC material and equipment, and AIS requirements are discussed.

MODULE 2

Computer Systems—This module covers computer hardware startup, including peripheral operations and system modification. Other topics discussed include computer center operations, media library functions, system operations, and troubleshooting techniques. Data file processes, memory requirements, and database management are also covered.

MODULE 3

Network Communications—This module covers network administration, LAN hardware, and network troubleshooting. Related areas discussed are network confilguration and operations, components and connections, and communication lines and nodes.

MODULE 4

Communications Hardware—This module covers various types of communications equipment, including satellites and antennas. Subjects discussed include hardware setup procedures, COMSEC equipment requirements, distress communications equipment, troubleshooting equipment, satellite theory, and antenna selection and positioning.

MODULE 5

Communications Center Operations—This module covers center operations, including transmit message systems, voice communications, center administration, quality control, and circuit setup/restorations. Guidelines for setting EMCON and HERO conditions and cryptosecurity requirements are also discussed.

CREDITS

Trademark Credits

Microsoft is a registered trademark of Microsoft Corporation.

INSTRUCTIONS FOR TAKING THE COURSE

ASSIGNMENTS

The text pages that you are to study are listed at the beginning of each assignment. Study these pages carefully before attempting to answer the questions. Pay close attention to tables and illustrations and read the learning objectives. The learning objectives state what you should be able to do after studying the material. Answering the questions correctly helps you accomplish the objectives.

SELECTING YOUR ANSWERS

Read each question carefully, then select the BEST answer. You may refer freely to the text. The answers must be the result of your own work and decisions. You are prohibited from referring to or copying the answers of others and from giving answers to anyone else taking the course.

SUBMITTING YOUR ASSIGNMENTS

To have your assignments graded, you must be enrolled in the course with the Nonresident Training Course Administration Branch at the Naval Education and Training Professional Development and Technology Center (NETPDTC). Following enrollment, there are two ways of having your assignments graded: (1) use the Internet to submit your assignments as you complete them, or (2) send all the assignments at one time by mail to NETPDTC.

Grading on the Internet: Advantages to Internet grading are:

- you may submit your answers as soon as you complete an assignment, and
- you get your results faster; usually by the next working day (approximately 24 hours).

In addition to receiving grade results for each assignment, you will receive course completion confirmation once you have completed all the assignments. To submit your assignment answers via the Internet, go to:

https://courses.cnet.navy.mil

Grading by Mail: When you submit answer sheets by mail, send all of your assignments at one time. Do NOT submit individual answer sheets for grading. Mail all of your assignments in an envelope, which you either provide yourself or obtain from your nearest Educational Services Officer (ESO). Submit answer sheets to:

COMMANDING OFFICER
NETPDTC N331
6490 SAUFLEY FIELD ROAD
PENSACOLA FL 32559-5000

Answer Sheets: All courses include one "scannable" answer sheet for each assignment. These answer sheets are preprinted with your SSN, name, assignment number, and course number. Explanations for completing the answer sheets are on the answer sheet.

Do not use answer sheet reproductions: Use only the original answer sheets that we provide—reproductions will not work with our scanning equipment and cannot be processed.

Follow the instructions for marking your answers on the answer sheet. Be sure that blocks 1, 2, and 3 are filled in correctly. This information is necessary for your course to be properly processed and for you to receive credit for your work.

COMPLETION TIME

Courses must be completed within 12 months from the date of enrollment. This includes time required to resubmit failed assignments.

PASS/FAIL ASSIGNMENT PROCEDURES

If your overall course score is 3.2 or higher, you will pass the course and will not be required to resubmit assignments. Once your assignments have been graded you will receive course completion confirmation.

If you receive less than a 3.2 on any assignment and your overall course score is below 3.2, you will be given the opportunity to resubmit failed assignments. **You may resubmit failed assignments only once.** Internet students will receive notification when they have failed an assignment--they may then resubmit failed assignments on the web site. Internet students may view and print results for failed assignments from the web site. Students who submit by mail will receive a failing result letter and a new answer sheet for resubmission of each failed assignment.

COMPLETION CONFIRMATION

After successfully completing this course, you will receive a letter of completion.

ERRATA

Errata are used to correct minor errors or delete obsolete information in a course. Errata may also be used to provide instructions to the student. If a course has an errata, it will be included as the first page(s) after the front cover. Errata for all courses can be accessed and viewed/downloaded at:

https://www.advancement.cnet.navy.mil

STUDENT FEEDBACK QUESTIONS

We value your suggestions, questions, and criticisms on our courses. If you would like to communicate with us regarding this course, we encourage you, if possible, to use e-mail. If you write or fax, please use a copy of the Student Comment form that follows this page.

For subject matter questions:

E-mail: n311.products@cnet.navy.mil
Phone: Comm: (850) 452-1501
DSN: 922-1501
FAX: (850) 452-1370
(Do not fax answer sheets.)
Address: COMMANDING OFFICER
NETPDTC N311
6490 SAUFLEY FIELD ROAD
PENSACOLA FL 32509-5237

For enrollment, shipping, grading, or completion letter questions

E-mail: fleetservices@cnet.navy.mil
Phone: Toll Free: 877-264-8583
Comm: (850) 452-1511/1181/1859
DSN: 922-1511/1181/1859
FAX: (850) 452-1370
(Do not fax answer sheets.)
Address: COMMANDING OFFICER
NETPDTC N331
6490 SAUFLEY FIELD ROAD
PENSACOLA FL 32559-5000

NAVAL RESERVE RETIREMENT CREDIT

If you are a member of the Naval Reserve, you may earn retirement points for successfully completing this course, if authorized under current directives governing retirement of Naval Reserve personnel. For Naval Reserve retirement, this course is evaluated at 3 points. (Refer to *Administrative Procedures for Naval Reservists on Inactive Duty,* BUPERSINST 1001.39, for more information about retirement points.)

Student Comments

Course Title: *Information Systems Technician Training Series*
Module 5—Communications Center Operations

NAVEDTRA: 14226 **Date**: _____

We need some information about you:

Rate/Rank and Name: _____ SSN: _____ Command/Unit _____

Street Address: _____ City: _____ State/FPO: _____ Zip _____

Your comments, suggestions, etc.:

Privacy Act Statement: Under authority of Title 5, USC 301, information regarding your military status is requested in processing your comments and in preparing a reply. This information will not be divulged without written authorization to anyone other than those within DOD for official use in determining performance.

NETPDTC 1550/41 (Rev 4-00

CHAPTER 1

CENTER OPERATIONS

Upon completing this chapter, you should be able to do the following:

- *Identify the procedures for transmitting messages via automated systems and manual circuits.*
- *Identify the procedures for monitoring and reporting of circuit backlogs.*
- *Identify the steps to verify broadcast number continuity.*
- *Determine the procedures for preparing, updating, and verifying the command guard list (CGL) and the master station log (MSL).*
- *Identify the procedures to verify STU-III systems parameters for remote/dial-in users and explain the need to set up and operate the STU-III terminals with remote/dial-in users.*
- *Determine the procedures for the preparation of the communications plan.*
- *Identify the steps to reset communications systems to RADAY.*
- *Determine communications protocols applied to circuit set up/restorations.*
- *List the steps to activate, deactivate, and place communications circuits in standby, set up, or restoration.*
- *Identify the procedures to transmit or receive cryptographic keying material via OTAT/OTAR.*
- *Define the steps to analyze network capacity and reliability.*

Telecommunications capabilities are continually advancing as technology improves. Because of advances in technology, we are seeing great improvements in the quality and speed of communications, and an increase in our information transfer capabilities. The Navy's modern automated systems greatly reduce writer-to-reader times in message handling, and the volume of messages that can be processed is steadily increasing.

ASHORE AUTOMATED TELECOMMUNICATIONS SYSTEMS

Two new shore command systems that are coming on-line in the 1990s are the Navy Standard Teleprinter Ashore (NSTA) and the Manual Relay Center Modernization Program (MARCEMP). We will discuss these two new systems as well as the other in-place automated shore systems and their interface components.

NAVY STANDARD TELEPRINTER ASHORE

With the introduction of the Navy Standard Teleprinter (NST) at afloat commands, there was a need to replace antiquated communications systems ashore with a system compatible with the NSTs. To meet this need, the Navy has developed the Navy Standard Teleprinter Ashore (NSTA) program.

The heart of the NSTA program is the Personal Computer Message Terminal (PCMT) and its

associated software. The PCMT (shown in figure l-l) is a PC-based microcomputer. The PCMT is a major step toward modernizing the entire Naval Telecommunications System.

Personal Computer Message Terminal

The Personal Computer Message Terminal (PCMT) is a remarkable military message-processing software package that runs on a combination of IBM-compatible PC- or AT-class desktop microcomputers and input/output devices called bus interface units (BIUs). The PCMT has the following advantages:

- For sites having a message relay requirement, the PCMT system eliminates handling torn paper tape.
- For small naval telecommunications centers (NTCs), the PCMT provides a sophisticated, easy-to-use automated message-handling system.
- For Local Digital Message Exchange (LDMX) or Naval Communications Processing and Routing System (NAVCOMPARS) subscribers that must be served remotely, the PCMT can provide an excellent, low-cost remote terminal capability. Received traffic can be reviewed at a terminal and selected messages shifted to a printer when a hardcopy is needed. The system will allow the operator to compose and save any number of partially completed pro forma messages. Subsequently, these messages can quickly and easily be retrieved, completed, and sent whenever needed.
- The PCMT allows messages to be exchanged via diskette media. For users who wish to exchange AUTODIN message traffic with their own PC-based systems, the PCMT provides an excellent vehicle for doing so.

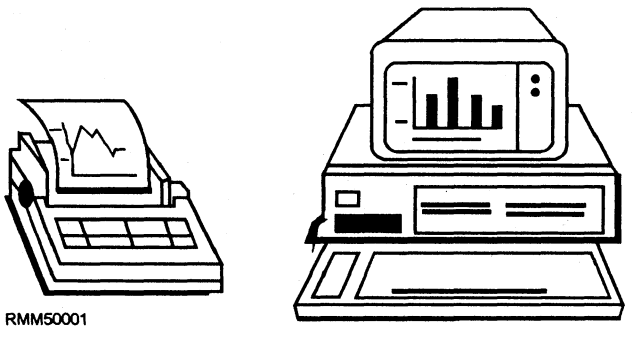

Figure 1-1.—Personal Computer Message Terminal (PCMT) with printer.

PCMT System

The PCMT message-processing system is a store-and-forward system that provides full accountability for all messages transmitted and received. The PCMT consists of a microcomputer configured with an 84-key keyboard, monitor, hard disk, and one or two floppy diskette drives. The PCMT also includes a medium-speed printer for printing message logs and hard-copy messages when required. Bus interface units (BIUs) are required to interface between the PCMT and the automated shore systems.

The PCMT microprocessor has 640K (minimum) of random-access memory (RAM) and uses the Microsoft® Disk Operating System (MS/DOS). The PCMT has a 5 1/4- and 3 l/2-inch disk drive capability. The minimum hard disk has a capacity of 10 million bytes. The hard disk varies based on software and user storage requirements. The PCMT may have either a nonremovable or removable drive, depending upon the user's security requirements.

The MS/DOS software is designed for a single workstation operation with operator-entered commands controlling the workstation. Powerful, easy-to-use message edit software will help the operator correct errors in input data from diskettes and generate messages. The monitors are monochrome except where the software has been coded to display pertinent information in color. In the next paragraphs, we will describe some of the capabilities of the PCMT.

The PCMT system assigns a message accountability number (MAN) to each complete or partial message processed. Once a MAN is assigned, the system reports each step in the processing of that message. This is done by automatically generated and on-demand log entries and on-demand message accountability reports. Message accountability reports identify all processing activity completed or pending for each message processed by the system.

The system also generates a log entry each time a complete or partial message is received, transmitted, or canceled. All messages received from or delivered to a diskette are further identified in the log entries and message accountability reports by the appropriate diskette volume identification.

The PCMT can be used to recall a specific message from the hard disk, which can be printed on an output

device. The operator can recall a message by providing a message accountability number (MAN), a component identification number (CIN), or a channel service number (CSN). The operator can also recall a message with an originating station routing indicator (OSRI), station serial number (SSN), or time of file (TOF).

The PCMT also provides significant paper reduction since information on receipt and delivery of message traffic is recorded on diskettes instead of paper. The PCMT stores messages on the hard disk until the operator requests delivery. The PCMT then outputs messages to a diskette, thereby reducing manual processing steps.

The PCMT system is setup so that narrative and data pattern (card image) traffic received from the serving LDMX and NAVCOMPARS can be delivered to the printer and/or diskettes. Data pattern traffic is usually delivered only to diskettes. Messages delivered to diskettes are segregated by routing indicators so that message centers receive only those messages addressed to them.

An operator can use the PCMT to enter a narrative or card image message, or create anew message using a simple keyboard/display screen editor. The terminal allows the operator to save a partially completed message on a diskette, recall it, and continue to edit it. At some communications centers, the operator can enter narrative or card image data pattern traffic prepared elsewhere.

Simple PC-based application programs that can be used in an office environment to review and prepare both narrative and card image messages are being developed. Once a day, the PCMT system will generate a summary report that identifies all traffic processed by the terminal during the previous 24-hour period.

The PCMT is the outgrowth of a program begun by COMNAVTELCOM (now COMNAVCOMTEL-COM) in 1982 to provide automation support for fleet message relay centers. The Navy had a continuing requirement to exchange message traffic over HF radio channels terminated at a relay site. Unfortunately, such channels impressed transmission garbles on any message they carried.

Since NAVCOMPARS required that message data presented by a TTY circuit be letter-perfect, NAVCOMPARS could not terminate such circuits directly. In the past, a message received on these circuits had to be punched out onto paper tape and printed simultaneously. The fleet center operator would then examine the printed copy and, if there were no errors, feed the paper tape into a reader that was on-line to NAVCOMPARS. If there was an error, either the ship would have to resend the message or the operator would have to recut the message's paper tape on a Model 28 TTY.

The process was slow, manpower intensive, and error prone. The system built in response to this need is now what we call the Manual Relay Center Modernization Program (MARCEMP).

MANUAL RELAY CENTER MODERNIZATION PROGRAM

The Manual Relay Center Modernization Program (MARCEMP) was first certified for operational use in 1988 as part of the NSTA program. However, even before certification, it was recognized that the system could serve as the basis for a much more generalized low-cost message-processing system. The typical MARCEMP system is a PCMT configuration.

The MARCEMP provides significant automation support for all aspects of HF message relay operations within the fleet. Since all HF fill-period termination and primary ship-shore traffic circuits have been terminated directly into a state-of-the-art computer-based system, the need to handle tom paper tape has been completely eliminated.

The MARCEMP system automatically checks formal messages for errors and sends them on when no errors are found. The system also makes available to a fleet center operator an advanced, full-screen computer terminal editor. The operator can use the terminal editor to correct format errors in the message that occur due to transmission garbles. The terminal editor can also be used to carry on an operator-to-operator dialogue with afloat communications personnel to coordinate corrective action.

The system provides a complete message audit trail and detailed accountability reports, which help ensure that all traiffic is properly handled. Its modular and flexible design permits it to be easily tailored to meet the varying individual needs of the large or small fleet center. MARCEMP can handle up to 24 send and 24 receive circuits simultaneously. MARCEMP can also process approximately 3,500 narrative or operator-to-operator dialogue messages daily.

A number of significant enhancements have been added to the MARCEMP version 1.0 baseline system. These enhancements have resulted in the PCMT version 2.0 as another configuration of the NSTA

program. This version is configured as a single workstation. Version 3.0 can be configured as a multiple workstation or single workstation PCMT system to replace both the earlier version 1.0 MARCEMP and version 2.0 PCMT. The PCMT version 3.0 can do everything MARCEMP and PCMT version 2.0 can do—and much more.

GATEGUARD SUBSYSTEM

The GateGuard subsystem is an Automatic Digital Network (AUTODIN) Interface Terminal (AIT) that provides user office automation systems (OASs) a gateway to the AUTODIN system. (AUTODIN is discussed later.) GateGuard also acts as a security guard device; hence, the name GateGuard. The GateGuard subsystem will eventually allow commands (subscribers) to interface directly with the AUTODIN system. This direct interface eliminates the manual handling of messages by the servicing telecommunications center (TCC).

Currently, a servicing TCC processes (transmit and receive) message traffic from the AUTODIN system for its subscribers. The GateGuard subsystem will eventually eliminate the need for TCCs because subscribers will be able to process their own messages through GateGuard. Subscribers will also be able to route messages via their local area networks (LANs) using desktop computers.

The GateGuard system is comprised of three elements:

- An AUTODIN Gateway Terminal (AGT),
- A gateway communications link to an Automated Information System (AIS), and
- A Guard Device (GD).

The AGT functions as a RIXT look-alike send-and-receive terminal connected to one of the AUTODIN subscriber terminals, such as the LDMX, NAVCOMPARS, or PCMT. The AGT serves as the primary AUTODIN interface point for a single organization.

The AGT has software that will operate on microcomputer systems designed to be operated by organization admin personnel. For example, in a small command, the AGT is located in the commanding officer's outer office and is operated by the Yeoman or secretary.

The communications link connecting the AUTODIN Subscriber Terminal (AST) with the AGT passes through the Guard Device (GD). The main purpose of the GD is to assist in enforcing system security policy. Specifically, the GD serves to isolate sensitive data in the serving AST from data processed by the AGT. It does so by ensuring that each message processed has been properly encapsulated and assigned a security code that the AGT is cleared to process.

The serving AST provides long-term archive storage for all messages sent to or received from the AGT. When the AGT is served by an LDMX, an operator at the AGT is able to recall messages from that system automatically. The operator is also able to identify the desired message by its originator and date-time group, originating station routing indicator, station serial number, time of file, or by the processing sequence number assigned to the message by that system.

The following is a simplified description of how the GateGuard subsystem works:

Various offices in a command have desktop computers that are interconnected by the command's LAN. Messages drafted on any computer in the system can be stored in a central computer. These messages can be accessed by any computer in the LAN. The messages can then be reviewed and checked for accuracy in format and content. When a message is released, the command sends it to the AUTODIN system via the GateGuard subsystem. At no time does the message leave the computer channels.

When messages are sent to subscribers via the AUTODIN system, the GateGuard subsystem will be able to identify messages for the various subscribers by plain language addresses (PLAs) or routing indicators (RIs). In some cases, GateGuard will use a key word or phrase in the message text to identify the subscriber for which the message is intended.

GateGuard will examine each message for which it accepts delivery responsibility, determine message completeness, and determine if it contains internally consistent security labels. If GateGuard detects any discrepancies, the software will not allow the message to be forwarded or delivered to a diskette. However, the message can still be routed to a local printer connected to the GateGuard subsystem.

AUTOMATIC DIGITAL NETWORK

The Automatic Digital Network (AUTODIN) is a worldwide computerized communications system. AUTODIN provides for the transmission of narrative and data pattern traffic on a store-and-forward basis.

AUTODIN provides reliable, secure, and efficient communications. AUTODIN also incorporates error detection and contains the highest speed transmission equipment currently available. AUTODIN is part of the Defense Communications System (DCS) and is managed by the Defense Communications Agency (DCA).

Interface equipments translate all AUTODIN inputs into common machine language, making AUTODIN compatible with many computer codes, speeds, and media, such as cards and tapes. Because of this, communications equipment within the NTS can be integrated into the AUTODIN system.

AUTODIN Switching Centers

The backbone of the AUTODIN system is the Automatic Switching Center (ASC). There are eight ASCs in the continental United States and five ASCs overseas (Europe and the Pacific).

The ASCs are interconnected into a digital network by trunk lines. Each center has local lines that link it to each subscriber (communications center) terminal. Messages entering the AUTODIN system at any of the subscriber terminals are forwarded through their respective switching centers. The ASCs accept messages from subscribers, determine the classifications and precedence of the messages, and relay the messages to the addressed subscribers.

AUTODIN Operational Modes

There are five AUTODIN system operational modes. These modes provide variation of speed and operation capabilities based on the equipment configurations of the message center subscribers. The following paragraphs describe each mode:

- **Mode I** —A duplex operation with automatic error and channel controls. Mode I operation allows independent and simultaneous two-way operation between two stations. The channel control characters acknowledge receipt of valid line blocks and messages or allow return of error information to the subscriber. The terminal (switching center) responds automatically to these characters by continuing or stopping transmission and displaying action information to the operator. A magnetic tape terminal is an example of terminal equipment using mode I.

- **Mode II** —A duplex operation normally associated with TTY or teleprinter equipments with independent and simultaneous two-way operation capability. There are no automatic error and charnel controls in mode II operation. Message accountability is maintained through channel sequence numbers and service message actions.

- **Mode III** —A duplex operation with automatic error and channel controls but only one-way transmission capability. The return is used only for error control and channel coordination response. The mode III channel is reversible on a message basis. Control characters are used in the same manner as in mode I.

- **Mode IV** —A unidirectional operation (send only or receive only) without error control and channel coordination. The mode IV channel is nonreversible and is equivalent to half-duplex operation of mode II.

- **Mode V** —A duplex operation, normally associated with TTY or teleprinter equipment, with independent and simultaneous two-way transmission. Control characters acknowledge receipt of messages and display limited information to the operator. Message accountability is maintained through the use of channel sequence numbers.

Input and output (I/O) devices, such as teleprinters, provide the central AUTODIN computer with the necessary means to communicate with the user. Output devices provide the means for changing the computer-processed data into a form specified by or intelligible to the users. The selection of I/O devices depends on the specific use for which a computer is intended.

Generally, I/O devices must meet several basic requirements. First, they must be able to modify all data so that it is acceptable to the computer during the input phase of the operation. The devices must also be able to present data in usable form during the output phase and operate quickly and efficiently with the computer.

I/O devices use coded languages. These languages are:

- **ASCII Code** —American Standard Code for Information Interchange, eight-level paper tape; and
- **ITA #2 Code** —American version of international TTY alphabet, five-level paper tape.

Message Header Programming

At the beginning of each AUTODIN message is a header (format line 2) containing pertinent information on the destination of the message. The originator can address a message either to a single addressee or to multiple addresses. This system saves time and requires fewer communications facilities, since only one message is prepared by the originator and sent to the switching center.

The timing system contained in AUTODIN equipment briefly connects a switching center to each subscriber terminal in turn. Computer memories act as reservoirs for the incoming messages of each subscriber terminal. The computer is programmed to connect each terminal in turn during a cycle. Messages received in their entirety are scheduled for output to the addressees' charnels as their turns arrive in the cycle.

AUTODIN has built-in safeguards that can detect almost any type of hardware or format error. Additionally, a complete (reference) copy of all relayed messages is kept on AUTODIN computer tape. A separate (journal) copy is made of only the addressee(s). Using this journal copy as an index enables the system to locate the reference copy of any message.

AUTODIN Tape Messages

The AUTODIN system is programmed to accept properly cut tapes and route them through the various switching centers and terminals en route to their ultimate destination. The system is then able to produce a tape and hardcopy for the designated addressee(s).

When preparing a message tape for the AUTODIN system, you must adhere to certain tape-cutting procedures. For example, format lines 1, 2, and 4 must not deviate; otherwise, the ASC will reject the message. The next paragraphs discuss the most important points on proper preparation of tape messages for transmission in the AUTODIN system.

ROUTING INDICATORS. —Within the AUTODIN network, a message tape is routed through the AUTODIN system to the addressee(s) by a routing indicator. Routing indicators are combinations of not less than four nor more than seven letters.

A routing indicator begins with the letter R or Q. The letter R indicates that the routing indicator is part of the worldwide tape relay system. The letter Q indicates that the routing indicator is within a self-contained network within a command or theater.

The second letter of the routing indicator identifies the nation or international alliance to which the indicator belongs. For example, the letter U refers to the United States. Therefore, RU indicates that the message tape is part of the worldwide network and is destined to a station in the United States.

The third letter of the routing indicator identifies the geographical area in which a particular station is located or from which it is served. This is necessary for relay purposes because the second letter may indicate a large nation within which there are a number of subdivisions or stations. For example, many stations in the United States are designated by the third letter C. Therefore, the first three letters of "RUC" indicate that the tape is part of the worldwide network, destined for the United States, and to a certain geographical area within the United States.

The fourth and subsequent letters of a routing indicator designate relay and tributary stations within the tape relay network. Like the first three letters, the fourth and subsequent letters may vary, depending upon location, area, and other factors.

TRANSMISSION IDENTIFICATION (FORMAT LINE 1). —As a means of maintaining traffic continuity, TTY terminals (modes II, IV, and V) must prefix each message header with a message transmission identification (TI). The ASC validates the elements in the TI. Modes I and III do not require format line 1. The TI is constructed without spaces and must be accurately prepared without corrections. For example, a correctly prepared TI might appear as follows:

VZCZCJTA (FIGS) 123 (LTRS) (2CR 1LF)

The elements of the TI and their meanings are as follows:

- **V** —Ensures that the first character of intelligence is not lost or garbled;
- **ZCZ** —Indicates the start of the message;

- **JTA** —Station/channel designator letters;
- **xxx** —Three-digit number indicating the sequential number of transmissions.

The station/channel designators vary for each channel and are determined by the status of the originating station. For example, if a minor relay or tributary station originates a TI to a major relay station, the first two characters consist of the fifth and sixth letters of the station routing indicator. The third character identifies the channel. Channel designators start with the letter A, progress alphabetically, and are assigned to all connected channels. For example, a tributary station having the routing indicator RUWTABA would use the designator "ABA" for the first outgoing channel and "ABB," "ABC," and so on, for additional outgoing channels.

MESSAGE HEADER (FORMAT LINE 2). —The message header is a basic 43-position header (figure 1-2). The message header is the starting point for the operator who is preparing the message tape. When preparing the header, the operator must remember that it must be letter-perfect.

The following paragraphs describe each position of the header:

Position 1 (Precedence) —The prosign Z (FLASH), O (IMMEDIATE), P (PRIORITY), or R

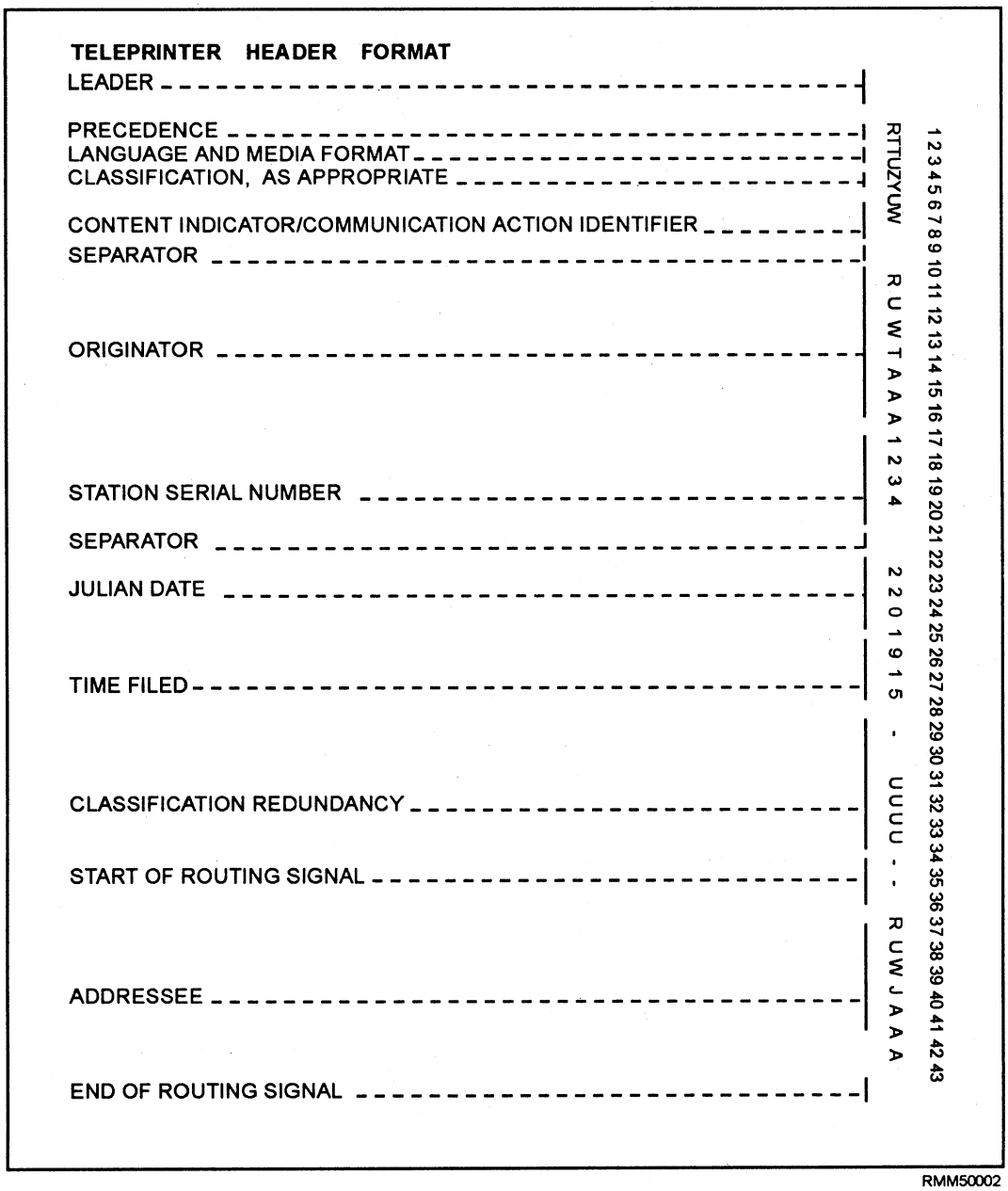

Figure 1-2.—Message header (format line 2).

(ROUTINE) is the first element. The prosign Y (YANKEE) is an emergency command precedence (ECP) and is assigned to emergency action messages (EAMs). The prosign Y indicates that a message has FLASH preemption capability. EAMs are processed ahead of all other traffic and interrupt lower precedence traffic already in processing within the AUTODIN system.

Positions 2 and 3 (Language and Media Format) —The language and media format (LMF) consists of two alphabetical characters. The LMF is the mode used to insert a message into the AUTODIN system. The LMF of the originating station is placed in position 2, and the LMF of the preferred output device of the addressee is placed in position 3. For example, in figure 1-2, positions 2 and 3 have the character T. The character Tin position 2 indicates that the originator's transmitting mode is paper tape (TTY/teleprinter) (five-level ITA2 code). The character T in position 3 indicates that the output device at the receiving end will be paper tape (TTY) (five-level ITA2 code). If the character C was used in position 3, this would indicate that the message was prepared and transmitted on paper tape and the output device at the receiving message center would be magnetic tape. *Automated Digital Network (AUTODIN) Operating Procedures,* JANAP 128, lists the LMFs used in the AUTODIN system.

Position 4 (Classification) —The letters authorized to indicate the message classification or special handling in this position are:

A	Special Category (SPECAT)
T	Top Secret
S	Secret
C	Confidential
E	Unclassified EFTO
U	Unclassified

Positions 5 through 8 (Content Indicator Code [CIC]/Communication Action Identifier [CAI]) —These positions of the header are a combination of either four letters or three letters and one number. These combinations are used to indicate message content and to provide identification for communications handling. For example, in figure 1-2, the CAI in positions 5 through 8 is ZYUW. This identifies the message as a narrative message. A CAI of ZFH2 would mean that the message is being forwarded to the addressee for information only. A CAI of ZYVW would indicate that the message is a service message. A complete listing of these codes is found in JANAP 128.

Position 9 (Separator) —At this point in the header, the operator must press the space bar to insert the TTYcode equivalent for space on the message tape.

Positions 10 through 16 (Originator) —The appropriate routing indicator of the originating station is placed in these positions.

Positions 17 through 20 (Station Serial Number) —The station serial number (SSN) of the sending station is inserted here. The SSN serves two specific purposes. First, when used in combination with the originator's routing indicator, it provides positive identification for each transmission. Second, in the end of message (EOM) validation (discussed later in this section), the SSN appearing in format line 15 provides a means by which the ASCs can check for the existence of straggler messages.

The SSN is expressed in four numeric characters, beginning with 0001 and continuing consecutively through 9999. A new series begins when the number 9999 is reached. Operating stations may use SSNs to identify local activities, channels, or positions within a station by assigning each activity a specific block of numbers. For example, one station may be assigned numbers 0001 to 2000; the next station 2001 to 4000, and so on.

Position 21 (Separator) —This position requires the same information as that for position 9.

Positions 22 through 24 (Julian Date) —The Julian date is the date that the message was received from the originator for transmission by the communications center. The first day of the calendar year is Julian 001, and each day is numbered consecutively thereafter.

Positions 25 through 28 (Time Filed) —The time filed is the time that the message was received from the originator by the communications center for transmission. Each filing time is expressed in Greenwich mean time (GMT) and must contain four numerical characters.

Positions 29 through 33 (Classification Redundancy) —For security reasons, the classification designator used in position 4 is repeated here. Position 29 is filled with a hyphen as a sentinel. The classification designator in position 4 is repeated in positions 30 through 33.

Position 34 through end-of-routing signal (start-of-routing signal and addressees) —The positions reserved for routing are made up of two sections: start-of-routing signal and the addressees' routing indicators. The start-of-routing signal consists of two consecutive hyphens and will always precede the first addressee routing indicator. Addressee routing indicators are listed immediately following the start-of-routing signal. A message can have a maximum of 500 routing indicators in these positions. If a message contains 501 or more routing indicators, the message will require two separate transmission. In this case, all routing indicators that have the same first four letters should be in one transmission

End-of-Routing Signal —The end-of-routing signal consists of a period (.) and is inserted in the position immediately following the last addressee routing indicator.

SECURITY WARNING (FORMAT LINE 4). —A security warning is the first component of format line 4. The appropriate operating signal (ZNR or ZNY) will always be followed by a classification character repeated five times. The operating signal and classification characters are as follows:

ZNR UUUUU —For off-line encrypted messages and classified messages transmitted in the clear;

ZNY EEEEE —For unclassified EFTO messages; and

ZNY, followed by CCCCC, SSSSS, or TTTTT —For Confidential, Secret, or Top Secret messages, respectively.

For SPECAT and SPECAT SIOP-ESI messages, the five redundant security characters are followed by an oblique (/) AAAAA for SIOP-ESI or BBBBB for all other SPECAT messages. For example, format line 4 for a Top Secret SPECAT message would be:

ZNY TTTTT/AAAAA(2CR, 1LF)

END OF MESSAGE (EOM) (FORMAT LINES 15 AND 16). —Format line 15 is the EOM validation line that is used to inhibit suspected straggler messages. Format line 15 consists of the SSN in format line 2 preceded by the number sign (#). Format line 16 consists of the EOM functions. The EOM functions consist of normal teleprinter ending procedure when five-level Baudot code is used (2CR, 8LF, 4Ns, 12LTRS). However, for ASCII, 12 delete functions are used (12DEL). The EOM for the message with format line 2 shown in figure 1-2 would be as follows:

TEXT	(2CR, 1LF)
BT	(2CR, 1LF)
(1FIGS)#1234(1LTRS)	
(2CR, 8LF)NNNN(12LTRS)	

Format lines 1, 2, 4, and 5 must all be accurately prepared. Backspacing, lettering out, double-spacing, or using two or more FIGURES and LETTERS functions in sequence will cause the ASC to reject the message during attempted transmission from the originating station. The EOM validation appearing in format line 15 and the EOM function in format line 16 must be prepared in uninterrupted sequence, be letter-perfect, and be without corrections.

General Teleprinter Rules

A leader must precede the header to ensure acceptance and transmission of the first character of the message header. The leader for the five-level Baudot code (most common) consists of at least six blanks and six letter functions. The leader for the ASCII (eight-level Baudot code) consists of at least six nulls and six delete functions. This will ensure acceptance and transmission of the first character of the message header.

When a message is assigned dual precedence, the higher precedence is shown in format line 2 (position 1). Both precedences are shown in format line 5.

Communications personnel of tributary stations must ensure that a record is made of the time of file (TOF) and the time available for delivery (TAD). These times are used to determine message-processing times.

Message Lengths

Messages cannot exceed more than 20 lines of heading and text, beginning with format line 5. Messages that exceed the 20-line limit must be divided into pages for transmission. The second and succeeding pages of a message are identified by the page number, the routing indicator of the station of origin, and the SSN. The security classification of classified messages follows the page identification. After the first letter of the classification, you must separate each letter by one space from the previous letter. For example:

PAGE 2 RUEDABA0123 C O N F I D E N T I A L (2CR, 1LF)

On unclassified messages, "UNCLAS" is placed after the page identification with no spaces separating the letters.

When a message exceeds five textual pages, the message must be divided into transmission sections. The message should be separated at a convenient point on the last permissible page of a transmission section. This normally will be at the end of a sentence or cryptopart. Each section must be numbered in plain language at the beginning of the text following the classification or abbreviation "UNCLAS." For example:

UNCLAS SECTION 1 OF 2

In long encrypted messages, when a transmission section starts with a new cryptopart, the designation of the cryptopart follows the designation of the transmission section. Also, when a numerical group count is associated with an off-line encrypted message and is indicated in format line 10, the count must indicate the number of groups in the textual section being transmitted— not the number in the complete message. Cryptopart identification is included in the group count; the page identification and transmission section are not.

Statistical and meteorological messages can have up to 100 lines of text without paging when the inclusion of paging information would disrupt processing by the user. However, you should divide these types of messages into transmission sections if they exceed 100 lines of text.

Misrouted and Missent Messages

A misrouted message is one that contains an incorrect routing instruction. This normally occurs when the originating communications center assigns an incorrect routing indicator during message header preparation. Misrouted messages are usually not discovered until they reach the communications center of the called routing indicator. Communications personnel of a tributary station in receipt of a misrouted message must take the following actions:

- Obtain the correct routing indicator, if possible;
- Apply a header change to the misrouted message and retransmit it to the correct routing indicator; and
- Originate a service message to the originating station advising of the reroute action and the correct routing indicator.

A missent message is one that contains a correct routing indicator but is transmitted to a station other than the one represented by the routing indicator. Missent messages can be caused by an equipment malfunction, incorrect switching, or operator error. Communications personnel of a tributary station in receipt of a missent message must take the following actions:

- Reintroduce the message into the AUTODIN system as a suspected duplicate (SUSDUPE) after applying a header change; and
- Forward a routine service message to the connected ASC citing the complete header and time of receipt (TOR) and advising that the message has been protected.

Suspected Duplicates

When a station suspects that a message may have been previously transmitted, but definite proof or prior transmission cannot be determined, the message should be forwarded as a suspected duplicate (SUSDUPE) by applying a header change. However, if a station receives a message that is already marked "SUSDUPE," the station should file the message if the message was previously received and delivered to the addressee. If there is no indication that the message was previously received and delivered, it should be forwarded.

Stations receiving unmarked duplicate transmissions should immediately forward a routine service message to the originating station. This service message should cite the complete header format of the duplicated message, including the TOR of the original and duplicate transmissions. If the initial copy was delivered to the addressee, the station should file the message.

Upon receipt of service messages concerning duplicates, communications personnel at the originating station must take the following actions:

- Check transmission records to determine the validity of the duplication report;
- Ensure that in-station procedures are adequate to guide operating personnel in the retransmission of SUSDUPE messages;
- Have maintenance personnel perform equipment checks if an equipment malfunction is suspected to be the cause of duplication; and

- Advise the connected ASC by routine service message if only one transmission can be accounted for.

An ASC receiving notification of a duplicate transmission should search its records to determine if the message was received in duplicate. If the message was not received in duplicate, it must be traced on a station-to-station basis to determine the point of duplication.

Magnetic Tape Messages

Magnetic tape is one of the principal media used in electronic data processing equipments (EDPEs). Magnetic tape terminal stations (MTTSs) in the AUTODIN provide for the rapid exchange of large volumes of data in a relatively short period of time. The basic mode of MTTS operation with other AUTODIN tributary stations is either full duplex or on a store-and-forward basis.

In the continental United States, terminals that have compatible equipment and circuit speeds and are connected to the same ASC may communicate directly by Hybrid AUTODIN Red Patch Service (HARPS). HARPS provides a direct subscriber-to-subscriber encrypted circuit. HARPS uses the same circuit and equipment normally used in the message-switching component of the network. Communications centers not serviced by HARPS communicate by normal message switching, which automatically performs the necessary speed, format, and code conversions.

Operating Rules

All received tape reels must be periodically dismounted and made available for delivery as scheduled by a receiving activity and system manager. A magnetic tape reel accepted by a communications facility for transmission is screened and arranged for transmission according to majority message precedence levels contained on the reel. Establishment of transmission schedules is the responsibility of the commands concerned. Prior coordination is necessary to provide for efficient use of the equipment and circuit time. Schedules are limited to 30 minutes per period.

Most facilities establish their own procedures for maintaining reel accountability and ensuring that message transmission has been accomplished. Message header and EOT printouts are finished by the message originator with each reel of tape to be transmitted. If a message cannot be transmitted, the MTTS operator returns the reel to the originator, identifying the message (or messages) that could not be sent. The originator is also provided the reason for the nontransmission, if known.

Terminal equipment should not be used to change message media format for customer convenience; for example, changing from magnetic tape to narrative records.

Operating Precautions

Communications station master records, such as history tapes and journal records, remain with the communications facility until destroyed. History tapes are labeled to prevent them from being inadvertently delivered to addressees with live traffic tapes.

Recorded information is very close to the edge of the tape. Tape-edge indentations, caused by careless tape handling, will seriously affect the accuracy of magnetic tape recordings. You should be aware that tape splices are not permitted in reels of tape used for traffic.

Message Formats

Message formats used within the AUTODIN require that each message contain a message heading, text, and EOT record. The textual material on magnetic tapes may consist of a wide variety of information recorded in either structured or nonstructured formats, depending upon the type of system.

EOT is either a single N or four consecutive Ns. The header, text, and EOT cards of magnetic tape messages are always transmitted in the AUTODIN common language code (ASCII). This is accomplished by automatic code conversion logic provided in the magnetic tape terminal.

The text of magnetic tape messages can be prepared by the EDPE system in 80-character data images, series record images, or by variable-length record images. The length of data records to be transmitted by AUTODIN may vary according to user requirements. For general transmission of data throughout the system, computerized terminals must be capable of transmitting records that contain from 18 to 1,200 characters.

Subscribers desiring to transmit messages that contain fewer than 18 or more than 1,200 characters must ensure that the addressee is capable of receiving such records prior to transmission. Typical line formats of magnetic tape message records are described in JANAP 128.

Magnetic tape messages prepared for transmission are limited to a maximum of 40,000 characters (five hundred 80-character data records) that include the header, text, and EOT records. The preparation of magnetic tape messages, formats, routing, contents, and sequence on tape is the responsibility of the message originator.

Message and Tape Reel Accountability

Each tape reel given to the MTTS operator for transmission must bear a tape label containing the following information:

- Reel number;
- Number of messages recorded on tape;
- Highest precedence used;
- Highest security classification;
- Date and time filed;
- Tape density;
- LMF used;
- Beginning and ending SSNs; and
- Time delivered to the MTTS operator.

Each blank reel of tape furnished to the MTTS operator for mounting on the receive tape transport contains a tape label with the following information recorded in the sequence of handling:

- A statement that the reel is blank;
- Reel number;
- Highest classification ever recorded;
- Time the reel is mounted on the receive transport;
- Time the reel is removed from the receive transport;
- Time the reel is delivered to the addressee; and
- Number and types of message on the reel and other applicable reel information.

All originated tape reels must be retained for at least 10 days. The header and EOT printouts finished the MTTS operator for both originated and terminated traffic are maintained as a station communications record for at least 30 days. Other logs recommended for MTTS operation are the master station log and the reel delivery log.

The master station log reflects the current operation status of the terminal equipments and circuits. This log should also reflect equipment and circuit outages, causes of the outages, and the corrective actions initiated.

The reel delivery log should indicate the reel number and the time the reel was delivered to the transmitting operator or the addressee.

AUTODIN Security

Required security protection must be extended to all classified traffic transmitted through the AUTODIN. The ASC automatically checks and compares the security classification stated in the header of the message against the authorized security level of the incoming circuit. Transmission of a message with a higher security level than authorized will result in the message being rejected by the ASC.

In addition, an automatic system-generated service will be transmitted by the ASC to the originating station. The purpose of this service is to advise the originating station of possible security compromises. Also, the ASC automatically checks and compares the security classification contained in the header of each message against the security classification of each destination. A security mismatch occurs for each destination that does not indicate a matching security level.

In the event of a security mismatch, the ASC takes the following actions:

- In a single-address message, the ASC rejects the message and alarms appear at the originating terminal indicating that the message needs retransmission.
- In a multiple-address message with at least one deliverable destination, the ASC accepts the message and delivers it to all valid destinations. For invalid routing indicators, an automatically generated service retransmits the message to the originating routing indicator and advises that the message needs retransmission.

In-station operating procedures should be carefully planned and rigidly enforced to prevent inadvertent transmission of classified messages to unauthorized stations or agencies. Complete security precautions and operating rules are contained in JANAP 128.

NAVAL COMMUNICATIONS PROCESSING AND ROUTING SYSTEM

The Naval Communications Processing and Routing System (NAVCOMPARS) is an automated system that serves as the interface between AUTODIN or other networks ashore and operational units of the Navy. There are five NAVCOMPARS sites: NCTAMS EASTPAC, NCTAMS WESTPAC, NCTAMS MED, NCTAMS LANT, and NAVCOMMTELSTA Stockton, California. The primary purpose of NAVCOMPARS is to provide security, speed, and systems compatibility for the Naval Telecommunications System (NTS). The NAVCOMPARS system provides the following services:

- On-line communications with AUTODIN switching centers;
- On-line communications with tactical and dedicated circuits;
- Off-line communications interface capabilities;
- Processing of JANAP 128-formatted messages;
- Conversion of DD Form 173 messages to JANAP 128 format;
- Conversion of modified ACP 126-formatted messages to JANAP 128 format;
- Filing, retrieving, and accountability of messages;
- Local delivery analysis;
- Distribution assignment;
- Message store-and-forward capability to fleet units;
- Fleet support through broadcast management or full-period terminations and primary ship-shore circuits;
- Broadcast keying and screening;
- On-line communications with the Worldwide Military Command and Control System (WWMCCS); and
- On-line communications with Common User Digital Information Exchange System (CUDIXS) and Remote Information Exchange Terminals (RIXTs). (CUDIXS and RIXT systems are discussed later.)

Automation of these functions and services eliminates manual processing and minimizes related delays and errors. Automation also improves originator-to-addressee delivery time and allows the timely exchange of information critical to the command and control of forces afloat.

LOCAL DIGITAL MESSAGE EXCHANGE

The Local Digital Message Exchange (LDMX) provides automatic outgoing message routing and reformatting for Navy activities ashore. It simultaneously transmits and receives messages over the AUTODIN and other remote terminal circuits. The LDMX system provides high-speed processing, system reliability, secure communications, flexibility, statistical information, and accounting data.

High-Speed Processing

The LDMX system provides high-speed communications processing. On-line to AUTODIN and other circuits, the LDMX system automatically receives, identifies, and files traffic for processing and future reference. Incoming messages are automatically arranged by precedence; then processed, edited, and printed on reproducible mats for delivery.

Outgoing traffic is entered by magnetic or paper tape. The system formats the outgoing message, creates a header, and validates the message identifiers, precedence, and classification. The LDMX system also searches system files to assign the correct routing indicator and arranges the message by precedence for automatic transmission. Operating at full capacity, the system can process up to 7,500 messages per day.

System Reliability

Message-processing reliability has been greatly improved by automatic message identification and header preparation and by system look-up files instead of manual files. The elimination of most manual functions and validation of those remaining greatly reduce misroutes and nondeliveries. The system continues to operate in either a semiautomatic or manual mode if a major component becomes inoperable.

Secure Communications

All message security fields are validated. If a mismatch is detected in the LDMX system, the message will be displayed to an inrouter or an outrouter for

review and action. Depending on user requirements, video display terminal (VDT) operators may be prevented from displaying or recalling Top Secret and SPECAT messages. The purpose of this precaution is to reduce the possibility of a security violation.

Flexibility

The LDMX system eliminates most manual processing without imposing stringent limitations on the user. Tailored to meet the unique situations at each command, the LDMX can be responsive to individual command requirements and variances.

Statistical and Management Reports

A significant feature of the LDMX system is the natural accumulation of statistical information and accounting data. This provides accurate verification of the reliability and performance of the system. Message-processing data is summarized in a series of statistical analysis summaries that include the following:

- A bar chart providing an hourly volume of incoming or outgoing messages;
- A summary report showing the number and average length of incoming or outgoing messages, the number of messages delivered to a remote printer, and the number of classifications and precedences;
- A listing of service messages sent and received;
- A listing of duplicated, misrouted, and missent messages; and
- A speed-of-service report, giving maximum, average, and minimum processing times (by precedence, classification, or selected originator).

FLEET COMMUNICATIONS SYSTEMS

The systems for afloat units are compatible with those used ashore. Next, we will discuss the types of automated systems used afloat.

NAVAL MODULAR AUTOMATED COMMUNICATIONS SYSTEM

The Naval Modular Automated Communications System (NAVMACS) is a shipboard message-processing system developed to meet command missions. The NAVMACS provides accurate, secure, and expedient communications for various classes of ships and flagships. The hardware, software, and fictional capabilities of the NAVMACS are based on the needs of individual ships and commands.

The current versions of NAVMACS are (V)1, (V)2, (V)2-MPD (message-preparation device), (V)3, and (V)5/(V)5A. NAVMACS capabilities are augmented in a building-block manner from the most basic system, (V)1, through the most sophisticated system, (V)5/(V)5A.

NAVMACS (V)1

The NAVMACS (V)1 configuration provides automation for the receipt and processing of up to four channels of incoming broadcast message traffic. This configuration provides one channel of incoming and outgoing high-speed satellite link message traffic from and to the CUDIXS (discussed shortly). The system incorporates the equipments and computer program necessary to perform the automatic address screening and management functions required in the processing of incomming messages. It also incorporates the storage, formatting, and accountability functions used in the ship-to-shore delivery of messages transmitted via satellite and the shore-to-ship delivery of messages received via broadcast and satellite.

NAVMACS (V)2

The NAVMACS (V)2 configuration provides the same message processing and delivery functions used in the (V)1 configuration for up to four channels of incoming broadcast message traffic. It provides one channel of incoming and outgoing high-speed satellite link message traffic from and to CUDIXS. The NAVMACS (V)2 configuration upgrades the (V)l system in the following ways:

- Adds automatic MILSTRIP paper tape message processing;
- Adds message output to medium-speed printers instead of low-speed printers; and
- Uses magnetic tape program loading instead of paper tape loading.

NAVMACS (V)2-MPD

The NAVMACS (V)2-MPD configuration has the same capabilities as the NAVMACS (V)2 version but uses a different program for operator language and

system printouts. The MPD program provides an additional capability for on-line message composition and editing ability, and outgoing message error analysis (before transmission). It also provides a proof copy with paper tape for off-ship transmission. The (V)2-MPD system consists of the same equipments as the (V)2 system with the addition of MPD units, which are modified video displays.

NAVMACS (V)3

The NAVMACS (V)3 configuration automates certain processing functions required in the handling of narrative messages. It serves as an afloat terminal within those communications networks using broadcast and point-to-point modes of operation on both conventional and satellite transmission paths.

The (V)3 configuration interfaces with up to four channels of fleet broadcast, and up to four channels of full-period termination send-and-receive circuits. It also interfaces with one channel of incoming and outgoing high-speed satellite link message traffic to and from CUDIXS.

The (V)3 configuration also interfaces with off-line torn tape and manual transmit/receive circuits of any type. The (V)3 system provides the capability of on-line message composition and on-line message retrieval fom magnetic tape.

NAVMACS (V)5/(V)5A

The NAVMACS (V)5/(V)5A system is an automated communications processing system capable of interfacing a mix of input/output channels. This system is enhanced with the addition of remote terminals for message input. It includes up to four incoming broadcast channels and eight itinerant, netted, and fully dedicated communication network channels. It also includes one incoming/outgoing high-speed satellite link with CUDIXS and onboard peripheral devices.

The (V)5/(V)5A system includes a remote terminal capability for direct input/output of narrative and data pattern messages to high-volume onboard user areas. Remote terminals consist of a medium-speed printer, video display, and paper tape reader/punch, or a combination thereof, depending on the unique requirements of the various remote terminals.

COMMON USER DIGITAL INFORMATION EXCHANGE SYSTEM

The Common User Digital Information Exchange System (CUDIXS) provides a bidirectional, ship-to-shore-to-ship, high-speed digital data communications link between a ship and a NCTAMS or NAVCOMMTELSTA. Subscriber stations use the NAVMACS as their terminal. The link consists of a single Fleet Satellite Communications (FLTSATCOM) half-duplex channel. The link is dedicated to synchronous communications between the CUDIXS shore station (Net Control Station (NCS)) and the subscribers afloat. Each CUDIXS communications link can operate with up to 60 subscribers. There are two types of subscribers: special and primary.

Special subscribers are those ships that are assigned subscriber identification (SID) numbers 1 through 10. Special subscribers can send and receive narrative traffic to and from CUDIXS.

Primary subscribers are assigned SID numbers 11 through 60. Primary subscribers are restricted to a send capability only. They can receive their shore-to-ship message traffic via other means, such as the fleet broadcast or fill-period terminations. Both types of subscribers can send or receive operator-to-operator (order wire) messages.

CUDIXS/Subscriber Net Cycle

CUDIXS/subscriber communications are accomplished through a modified round robin network discipline. The basic round robin net operating concept transfers net control from one subscriber to the next on a prearranged basis, completing one net cycle when each participating subscriber has transmitted.

In the CUDIXS/subscriber modified round robin operating concept, transmission timing and scheduling are determined solely by the CUDIXS shore station designated the NCS. Each net cycle starts when the NCS transmits a Sequence Order List (SOL) along with narrative traffic and operator-to-operator messages. The SOL specifies the order in which each subscriber transmits during the next net cycle and the amount of time allocated each transmission slot. Each subscriber, in turn, will transmit at a time computed from information in the SOL.

A net cycle can range from 20 to 120 seconds, depending upon the amount of transmit time requested by the subscribers and the amount of data transferred.

System Performance/Message Accountability

CUDIXS provides a shore operator with several means of monitoring system performance and maintaining message accountability for all messages processed by the CUDIXS NCS. Specifically, the system assigns sequence numbers to all messages processed, provides link status, traffic statistics, and system summary information in system reports. The system also allows the operator to assign parameter values that control net operations and to generate various alerts concerning immediate communications difficulties.

System Interfaces

CUDIXS serves as an extension of AUTODIN by storing and forwarding messages, normally without need for human intervention. CUDIXS interfaces with AUTODIN via the NAVCOMPARS and processes narrative traffic for general fleet communications teleprinter messages.

In accomplishing its tasks, CUDIXS supplements the traffic responsibilities previously assumed by ship-to-shore and broadcast HF circuits. CUDIXS can recognize EMERGENCY COMMAND, FLASH, IMMEDIATE, PRIORITY, and ROUTINE messages on a first-in-first-out (FIFO) basis within precedence. Through system reports, the operator has the following capabilities:

- Detailed information on every message processed by CUDIXS;
- Overall statistics on the volume of message traffic processed over the link; and
- Information on the quality of link communications with each net subscriber.

COMMUNICATIONS DATA PROCESSING SYSTEM

The Communications Data Processing System (CDPS) provides the USS *Tarawa* (LHA-1) class ships with the necessary communications hardware and software to process narrative traffic and to ensure circuit reliability. CDPS is one of the most complex of the automated systems afloat and offers the following capabilities:

- Automatic broadcast screening;
- Frequency management;
- Automatic message logging;
- Automatic message continuity checks;
- On-line message preparation and storage;
- Backup control and operation;
- High-speed data interface;
- On-line operational readiness testing;
- Quality monitoring with computer aid;
- Message error analysis;
- Circuit status and record-keeping functions;
- Construction of communications circuits; and
- Ability to act as a CUDIXS special or primary subscriber.

As with many of the automated systems, the operator has the ability to modify system configuration from the control console. The operator must know how to properly use, operate, and perform system changes. Your job will involve setting up and operating input/output (I/O) devices. Some systems allow the operator to patch receivers, transmitters, modems, and antennas directly from the console.

As a Radioman, part of your routine duties will be to energize electronic equipment and monitor power levels. In the event of primary power failure, equipment must be brought up on emergency or back-up power systems. Many of the automated systems in use today have uninterrupted power sources (UPS) or battery backups to preclude a complete system failure.

For more information on power requirements for individual components, refer to the equipment technical or operator manuals. You should become familiar with emergency power requirements and procedures **prior** to an actual emergency.

SUBMARINE SATELLITE INFORMATION EXCHANGE SUBSYSTEM

The Submarine Satellite Information Exchange Subsystem (SSIXS) provides the commanding officers of SSN and SSBN submarines with an optional satellite path to complement existing VLF/LF/HF broadcasts. The subsystem provides a rapid exchange of teleprinter information between SSN and SSBN submarines and shore stations.

To use the SSIXS, the submarine must be in a line-of-sight position with a satellite. The submarine must also be in a tactical situation that permits exposure of its mast-mounted antenna.

The SSIXS provides access to a satellite path through a programmable mixture of query-response and broadcast-without-query functions. This type of access provides maximum operational flexibility to the submarine commander.

All transmissions on the SSIXS provide automatic, reliable, long-range, high-data-rate, and cryptographically secure UHF communications between submarines, and between submarines and shore stations.

AUTOMATED VOICE COMMUNICATIONS SYSTEMS

The telephone is and will continue to be a convenient and fast way to communicate. In this section, we will discuss the Secure Telephone Unit Third Generation and the Defense Switched Network (DSN), which is an updated version of the Automatic Voice Network (AUTOVON).

SECURE TELEPHONE UNIT THIRD GENERATION

The Secure Telephone Unit Third Generation (STU-III) is the newest communications system that meets the need for protecting vital and sensitive information over a telephone system. The STU-III is a compact, self-contained desktop unit capable of providing the user with clear and secure voice and data transmissions. The unit is fully TEMPEST protected and is certified by the National Security Agency for use up to and including Top Secret material.

The STU-III is unique in that it works as an ordinary telephone and as a secure telephone network to other STU-III terminals. For secure transmissions, the STU-III uses a unique keying system.

The three manufacturers of the STU-III terminals for the Navy are AT&T, Motorola, and General Electric. Figure 1-3 shows an AT&T STU-III terminal.

The STU-III is operated the same as any telephone. That is, you pick up the handset, wait for a dial tone, then dial the number of the person you want to call. All calls on the STU-III are always initiated in the clear voice mode. Once the party you have called has answered, you have the option of talking to that person in the clear voice mode, clear data mode, secure voice mode, or the secure data mode.

Terminal Setup

The STU-III terminal uses special keys with a designator of KSD-64A. The KSD-64A is a plastic device that resembles an ordinary key. Two types of keys are used with the STU-III, the seed key and the crypto-ignition key (CIK). The seed key is a special keying material used for the initial electronic setup of the terminal. The CIK key is used by the users to activate the secure mode.

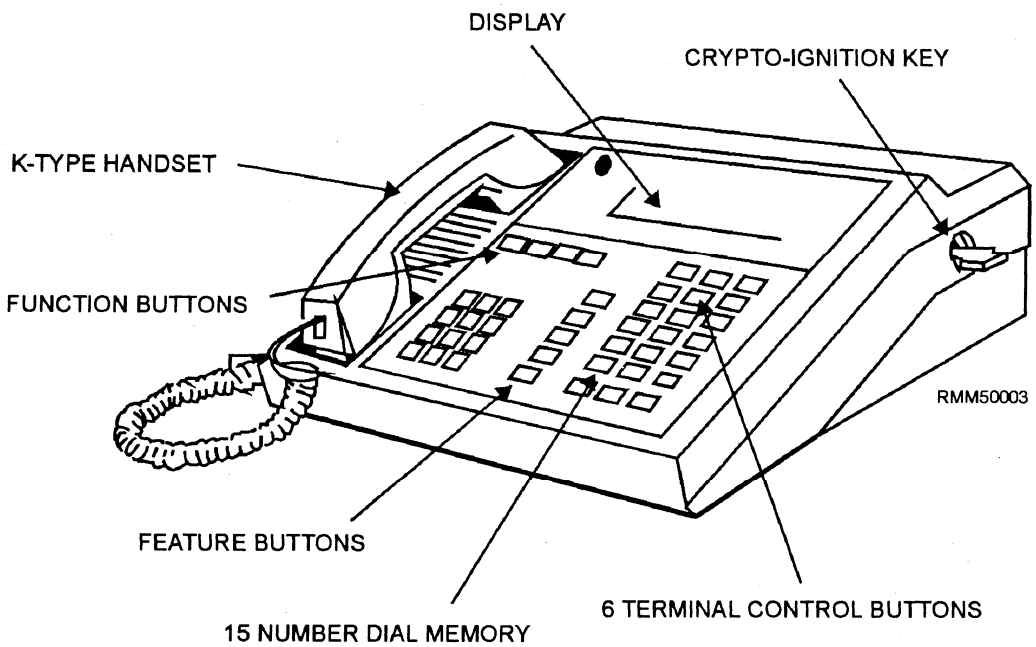

Figure 1-3.—AT&T STU-III terminal.

When the STU-III terminal is installed, the STU-III custodian sets up the terminal with the seed key. A seed key is issued to a particular terminal only. The seed key contains a microchip that is embedded electronically with identification information. This information includes the level of security authorized for that terminal.

Once the custodian inserts the seed key into the terminal, the information on the key is transferred to the internal memory of the terminal. At this point, the seed key no longer contains any information and is considered to be "empty."

The information in the terminal is electronically registered with the Key Management Center (KMC) located in Finksburg, Maryland. The KMC is the central authority responsible for controlling the key material and issuing reports of compromised keys. The user can discuss classified information up to the security level that has been keyed to the terminal.

The crypto-ignition keys (CIKs) can now be made for users to activate the secure mode. The CIKs are "empty" keys with no information embedded in the metal strip. When the empty keys are inserted into the terminal, some of the information that is now stored in the terminal from the seed key and other information in the memory is transferred onto the metal strips. This information becomes an electronic "password" on the CIKs for that particular terminal, making the CIKs unusable on other terminals. The terminal maintains a list of authorized CIKs for each key in its memory.

When using a STU-III with remote or dial-in, users parameters will be set according to the Secure Telephone Unit Third Generation (STU-III) COMSEC Material Management Manual (CMS 6) and locally generated instructions.

Levels of security classification, keying instructions, rekey instruction, CIK management will be decided by the user and the user's communications facility. All users must meet the minimum security clearance requirements.

Training on the STU-III will be documented in accordance with CMS 6 and local instructions.

Secure Mode

As we mentioned earlier, the secure mode of the STU-III is activated and deactivated using a CIK. When the CIK (figure 1-3) is inserted into the terminal, the STU-III can be used in the secure mode up to the classification of the keying material. Without the CIK, the STU-III operates as an ordinary telephone.

Calls are always initiated in the clear. To go from a clear to a secure voice transmission, either caller simply presses his or her SECURE VOICE button after the CIK is used to activate the secure mode.

Once a secure link has been initiated, the two STU-III terminals begin exchanging information. The information exchanged includes the identity of the CIK of the distant-end person, the list of compromised CIKS, and the common level of classified security information to which the two callers have access.

When two terminals communicate in the secure mode, each terminal automatically displays the authentication (identification) information of the distant terminal. This information is scrolled through the display window during secure call setup. The first line of the identification information and the classification are displayed for the duration of the secure call.

The information displayed indicates the approved classification level for the call, but does not authenticate the person using the terminal. Each terminal user is responsible for viewing this information to identify the distant party and the maximum security classification level authorized for the call.

STU-III Administration

The STU-III terminals and keys are COMSEC material. The terminals and keys may be administered either through the STU-III custodian or the CMS custodian. Both the terminals and keys are issued to users and must be signed for. Since the seed key is classified, it must be afforded protection for the level of classification in accordance with *Secure Telephone Unit Third Generation (STU-III) COMSEC Material Management Manual,* CMS 6.

Because CIKs permit the STU-III terminals to be used in the secure mode, the CIKs must be protected against unauthorized access and use. CIKs may be retained by the users who sign for them on local custody. Users must take precautions to prevent unauthorized access and must remember to remove the CIKs from the associated terminals.

When the terminals are unkeyed, they must be provided the same protection as any high-value government item, such as a personal computer. When the terminal is keyed, the terminal assumes the highest classification of the key stored within and must be protected in accordance with the classification of that key.

DEFENSE SWITCHED NETWORK

The Defense Communications System (DCS) Defense Switched Network (DSN) is a telecommunications telephone interconnected network. This system is found on most military and other Federal Government installations in the United States and overseas.

This system upgraded the Automatic Voice Network (AUTOVON) and will evolve into an all-digital network in the 1990s. The DSN incorporates capabilities that were not available in the AUTOVON system, such as automatic callback, call forwarding, call transfer, and call waiting.

Precedence of Calls

The precedence of a call indicates the degree of preference to be given a call relative to all other calls in progress. A preemption feature provides the ability to disconnect a call of lower precedence and seize the access line or interswitch trunk to complete a call of higher precedence. A unique aspect of the DSN is that switches have been programmed to determine what precedence treatment must be given each call.

The combined features of precedence and preemption used in DSN are called multilevel precedence and preemption (MLPP). The effectiveness of this system depends on the proper use of the precedence system by the users.

All users should be familiar with the system and the types of calls assigned to each precedence. Each user should ensure that his or her call is not assigned a precedence higher than that justified by the circumstance or information involved.

The DSN offers five types of call treatment. The precedences and their applications are listed below in relative order of priority in handling.

FLASH OVERRIDE (FO) —FO takes precedence over and preempts all calls on the DSN and is not preemptible. FO is reserved for the President of the United States, Secretary of Defense, Chairman of the Joint Chiefs of Staff, chiefs of military services, and others as specified by the President.

FLASH (F) —FLASH calls override lower precedence calls and can be preempted by FLASH OVERRIDE only. Some of the uses for FLASH are initial enemy contact, major strategic decisions of great urgency, and presidential action notices essential to national survival during attack or preattack conditions.

IMMEDIATE (1) —IMMEDIATE precedence preempts PRIORITY and ROUTINE calls and is reserved for calls pertaining to situations that gravely affect the security of the United States. Examples of IMMEDIATE calls are enemy contact, intelligence essential to national security, widespread civil disturbance, and vital information concerning aircraft, spacecraft, or missile operations.

PRIORITY (P) —PRIORITY precedence is for calls requiring expeditious action or furnishing essential information for the conduct of government operations. Examples of PRIORITY calls are intelligence; movement of naval, air, and ground forces; and important information concerning administrative military support functions.

ROUTINE (R) —ROUTINE precedence is for official government communications that require rapid transmission by telephone. These calls do not require preferential handling.

Security

Local command policy normally states that the DSN is to be used only for the most essential official calls. The DSN system must never be used to make personal or unofficial calls.

Telephone circuits, particularly those routed by high frequency and microwave, are susceptible to monitoring and interception. **The DSN is not a secure system!** Users must take care and use common sense to avoid divulging classified information. Giving hints or talking "around" a classified subject can lead to the compromise of classified information.

TRANSMIT MESSAGES VIA MANUAL CIRCUITS

In these days of super speed burst message transmission the use of manual relaying or transmitting of messages is not the norm. You should locate, identify, and use locally produced instructions, publications, and references.

ENEMY CONTACT REPORTING

Enemy contact reports are normally made only once when you are in direct communications with the officer in tactical command (OTC), a higher authority, or a shore radio station. Enemy contact reports are signaled using basic R/T procedures as modified by chapter 6 of ACP 125. Details of enemy contact

reporting are contained in *Allied Maritime Tactical Instructions and Procedures,* ATP 1, Volume I. There are two conditions under which enemy contact reports are to be made more than once:

- When DO NOT ANSWER procedures are used (texts are transmitted twice in this procedure).
- When the text consists of emergency alarm signals. In this case, the text is transmitted twice, separated by the proword I SAY AGAIN, with a time group in the ending.

When required, authentication is used in contact reports. Lack of proper authentication, however, should not prevent retransmission or relay of the message to higher authority.

There are two types of contact reports: initial and amplifying. As you would expect, initial reports are used to report initial contact or sightings. These reports should be sent as expeditiously as possible with immediate, pertinent information (type vessel, location, basic track, and so forth). The amplifying reports contain all necessary amplifying information to be fully analyzed by higher authority or command.

CODE AND CIPHER MESSAGES

Code words, such as VERDIN in the text EXECUTE PLAN VERDIN, are sent as plain language words. Encrypted groups, such as DRSRM, are spelled phonetically: DELTA, ROMEO, SIERRA, ROMEO, MIKE.

The phonetic alphabet is used for the names of signal flags as well as for spelling words, letter groups, and so on. Signal flags are combined into code groups that have meanings of their own. DELTA ROMEO ONE, for example, might mean "prepare to hover." Signal flag A is ALFA, flag B is BRAVO, and so on. Meanings of such code groups are given in appropriate signal publications.

Because flag signals are also sent by R/T, you must be able to differentiate between the two uses of the phonetic letters when you hear them. Here is the way—if the phonetic alphabet is used, the proword I SPELL precedes it and each phonetic letter is recorded as a letter. If you hear I SPELL, followed by DELTA OSCAR, write it as DO. On administrative nets, the proword SIGNALS, followed by DELTA OSCAR, means the groups have been taken from a signal book and should be recorded as such. Prowords are not used on nets used primarily for conveying signals. Therefore, you may assume that alphabet flags are intended.

The duties of an R/T operator require a knowledge of the special language developed for tactical maneuvering, air control, antiair warfare, naval gunfiie support, electronic countermeasures, antisubmarine warfare, and other specialized uses. Words, phrases, and abbreviations used in R/T for these specialized uses are called operational brevity codes. A complete list of operational brevity code words is found in *Operational Brevity Codes,* ACP 165.

You should understand that the words and phrases of the brevity code provide no communications security. The purposes of the codes are to:

- Standardize the vocabulary;
- Improve the accuracy of the transmission; and
- Shorten transmission time.

AUTHENTICATION

Authentication is a security measure designed to protect a communications system against fraudulent transmissions. There are specific times when you will have to use authentication procedures. Several types of authentication systems are in use, and the method of authentication will vary with the system that you are using. Authentication systems are accompanied by specific instructions outlining the method of use. You can find more information about the types of authentications and specific reasons when and why to use the authentication process in *Communications Instructions—Security (U),* ACP 122, and in NTP 5.

COMMUNICATIONS CENTER ADMINISTRATION

We will now show you some of the basic logs, command guard list (CGL), and changing call signs that deal with communications center administration. These short instructions are in no way a complete list of communications center operations. Each command has its own check-off lists or SOPs of how their command runs its center.

CIRCUIT BACKLOGS

Each circuit operator will notify the supervisor when the circuit status changes, when a backlog of traffic develops, when an outgoing transmission is delayed, or when any deviation from prescribed

procedures is recognized. Circuit operators will report the backlog or potential for backlogs (logged-out equipment, poor reception) to the supervisor, who will in turn pass the information up the chain of command to the CWO and will also log the information into the master station log (MSL).

When relieved, the circuit operator will pass on information pertaining to the circuit(s), when it is not covered in the circuit status standard operating procedures.

A broadcast form provides for the number of messages received, the classification of the message, and also provides a record of destruction for classified message traffic. A check-off sheet (stock number 0196-LF-301-2350) is available through the supply system for keeping a record of broadcast numbers received and transmitted.

COMMAND GUARD LISTS

Each command is responsible for maintaining an accurate list of all AIGS, CADS, general messages, and task organization assignments required to fulfill its mission, and to supply this guard list to a serving communications center.

The command guard list must be verified with the communication plan to ensure that it is accurate and any discrepancies are corrected prior to updating. This is normally done when a change in tasking, operating area, or mission occurs.

DAILY CALL SIGNS

FLTCINC communications operating plan will prescribe the specific form of call sign to be employed based on the network used and operating conditions.

Call signs are to be used when first establishing a net, when reporting into a previously established net, and in the transmission and address components when a message is required to be relayed to a station that is on a different net.

Daily call signs, by their very name, direct you to change the call signs daily, using various issued publications. Refer to local operating instructions for instructions on how to verify the type of daily call signs you are using for specific situations.

MASTER STATION LOG (MSL)

The MSL is the official narrative record maintained to record significant events (e.g., power failures, complete system outages, major equipment outages or impairments such as HAZCON'S and any other event that may have an impact on operations, time verification, shift or watch changes, special tests, etc.). Every communication space must maintain a Master Station Log.

Entries must be made in chronological order. The shift or watch supervisor is required to sign the log when logging "on" and "off" duty and at the end of the RADAY.

If the MSL is an automated log, it shall be designed so that it does not allow alternations. For manual logs, a hard copy of the MSL must be filed at the end of each RADAY. MSLs must be retained for a minimum of 12 months.

THE COMMUNICATIONS PLAN

The communications plan satisfies the communications requirements of an operation. It specifies circuits, channels, and facilities to be used and stipulates the policies and procedures that are applicable. The plan is, in effect, an assignment of communications tasks to be performed by subordinate commanders or by supporting commands.

The planner first establishes requirements for communications and then determines the best means for satisfying them. This process may reveal shortages or inadequacies in what is available. If inadequacies are identified, it may become necessary to share circuits or facilities, as well as to merge or consolidate requirements. All possibilities should be considered to support valid operational requirements.

In planning communications, the planner must evaluate such factors as the performance, capabilities, and capacities of systems and facilities, as well as the personnel. These factors are merely guides and averages. They represent the sum result of experience in previous similar situations, and are considered only after any local factors are determined. These factors change from time to time and must all be available for final determination of communications requirements.

QUALITY CONTROL

The AN/SSQ-88/A/B system was designed to provide a means of monitoring and evaluating performance of any communications system used by forces afloat. You will utilize this system with RCS interface as well as various other types of monitoring systems; for example, oscilloscopes, meggers, and visual, just to name a few.

You will be checking for various signal quality characteristics, including dc distortion, audio distribution levels, frequency accuracy of RF signals, spectrum analysis and loop current. Those measurements are broad categories and can be broken down to specific tests for specific systems.

You will correct all discrepancies, complete the appropriate reports, and send them to the proper authority or file them for further reference.

CIRCUIT SETUP/RESTORATIONS

RADAY is the start of a new 24-hour period. At that time all designated systems will restart. It can be a crypto restart, the simple methods of starting (opening) a new log, or message numbering system, starting at the number 0001.

RADAY starts at 0001Z worldwide. The 0000Z time frame does not exist and **WILL NOT** be used. The following restart items is a rudimentary list to give the user an idea of areas and items that require restart at the beginning of the new radio day.

DETERMINE COMMUNICATIONS PROTOCOLS

Protocols are generally set by the CINCs, area commander, Naval instructions, and local instructions. Protocols are also determined by the mission and the area of operations.

COMMUNICATIONS CIRCUITS

The use of communications circuits require that those circuits at various times of the day be placed online, in reserve, or taken offline. The reasons have to do with whether the circuit is needed immediately, or can be placed on ready reserve for use, or if the requirement for that particular circuit has expired.

Activate

Activating communications circuit usually means turning on or starting a circuit to allow for communications signals to ride (or pass) on them. When a circuit is activated, it will be logged in an active status on the status board. A circuit can be activated for any number of reasons, including special communications, overload, or installation of a new circuit path.

Deactivate

To terminate or deactivate a circuit is to stop using that path and remove all your equipment from that particular path. The deactivated circuit is then logged out on the status board.

Standby

By placing communications circuits standby, you are placing them in hold. They are ready for activation or deactivation should the need arise. Again, this type of circuit is placed on the status board so that the supervisor knows the status of each of the circuits under his control.

SHIFT FREQUENCIES

Shifting frequencies or changing frequencies is accomplished to allow for stronger propagation of the circuits. When the signal strength begins to decay, the operator will shift frequencies to another or stronger frequencies in accordance with naval and local instructions.

TRANSMIT OR RECEIVE CRYPTOGRAPHIC KEYING MATERIAL VIA OTAT/OTAR

Some of the new cryptosystems will use a 128-bit electronic key that is called over-the-air-rekey (OTAR) or over-the-air transfer (OTAT). Using this system reduces the amount of physical keying material held on board a command.

The key can be extracted using a KYK-13 or KYX-15/KYX-15A. The key is then loaded into another cryptosystem.

For amplifying information, refer to *Procedures Manual for Over-the-Air Transfer (OTAT) and Over-the-Air Rekey (OTAR) and Field Generation and Over-the-Air Distribution of Tactical Electronic Key*, NAG-16/TSEC.

ANALYZE NETWORK CAPACITY AND RELIABILITY

When trying to analyze a network's capacity and reliability, you must first establish the criteria or level at which you wish the system to work. Does the network have set boundaries, or can it be expanded to include updated or new parameters? Many avenues can be

explored to find the most efficient methods and levels at which a network can work.

Accurate documentation is a key factor for showing the user what, where, total numbers, and reliability of the network.

You will find that with the correct numbers you can see where a system or network is falling short or surging ahead of the set projection data.

SUMMARY

In this chapter you have been introduced to communications systems, networks, and administration concerns in their most basic forms.

Not all of our work is concerned with strategic or tactical operations. Establishing circuits or networks, quality control, and the various operations of the STU-III are just a few of the many facets of our complex and diverse jobs.

CHAPTER 2

VOICE COMMUNICATIONS

Upon completing this chapter you should be able to do the following:

- *Identify circuit procedures, discipline, and techniques in voice communications.*
- *Describe radiotelephone (R/T) security elements, voice procedures, and basic message formats.*
- *Explain the use of R/T call signs, circuits, and nets.*
- *Explain the use of R/T executive methods.*
- *Identify the use and format for R/T circuit logs.*

Whether you are ashore or at sea, your professional duties as a Radioman will include radiotelephone (R/T) communications. You should understand that uncovered (nonsecure) radio transmissions are the least secure means of communications, and that R/T voice communications are the least secure of all radio communications. Despite these drawbacks, R/T communications play an important part in our day-to-day fleet operations and in the control of coastal and harbor shipping.

CIRCUIT PROCEDURES

R/T is the easiest, most convenient method of relaying real-world situation traffic from ship to ship, ship to shore, or shore to ship. All that is necessary is that you pick up a transmitter handset and speak into it.

A radiotelephone circuit would quickly become unusable if everyone on the circuit failed to follow the same rules and procedures. Much of what is accomplished over an R/T circuit involves proper techniques and training, coupled with common sense and experience. It is impossible to cover every conceivable situation that may arise when using voice communications. There are many simple R/T procedures that apply to these circuits.

CIRCUIT DISCIPLINE

Unless using secure voice communications equipment, you must assume that everything you say when using R/T is being intercepted. The inherent dangers of interception can be significantly reduced by adhering to the principles of strict circuit discipline.

R/T transmissions should be as short and concise as possible without sacrificing clarity. It is important that all personnel using voice communications be instructed in the proper use of the handset and R/T equipment. They must also be cautioned on the likelihood of transmission intercept.

Adherence to prescribed operating procedures is mandatory! Deviations from these procedures create confusion, reduce reliability and speed, and tend to nullify security precautions. Once you know the proper operating procedures, you can use your initiative and common sense to satisfy specific operating requirements.

Although circuit discipline is discussed here with respect to its connection with R/T procedures, you must understand that the requirement for circuit discipline applies to all communications circuits—not just R/T circuits. Every operator must recognize and avoid the following malpractice, which could endanger communications security:

- Linkage or compromise of classified call signs and address groups by plain language or association with unclassified call signs;
- Linkage or compromise of encrypted call signs and address groups by association with other call signs, address groups, or plain language (for example, use of encrypted call signs in the call and unencrypted call signs in the message address);
- Misuse and confusion of call signs, routing indicators, address groups, and address indicating groups (AIGs) (which could result in the nondelivery of an important message, a compromise, or the linking of classified and unclassified call signs and address groups);
- Violation of emission control (EMCON) conditions;
- Unofficial conversation between operators;
- Transmitting on a directed net without permission;
- Transmitting the operator's personal sign;
- Excessive repetition of prowords;
- Use of plain language in place of applicable prowords;
- Unnecessary transmissions;
- Incorrect and unauthorized procedures;
- Identification of unit locations;
- Excessively long calls (when a station is called and does not answer within a reasonable time, presumably because a condition of radio silence prevails, the message may be transmitted in the blind or by some other method);
- Use of profane, indecent, or obscene language; and
- Failure to maintain radio watches on designated frequencies and at prescribed times.

CIRCUIT TECHNIQUES

You should use the following guide in developing good voice circuit techniques. To enhance your proficiency, you should practice the techniques on a training net. Remember, though, that nothing can take the place of good common sense.

DO:

- Listen before transmitting. Unauthorized break-in causes confusion and often blocks a transmission in progress to the extent that neither transmission gets through.
- Speak clearly and distinctly. Both slurred syllables and clipped speech are hard to understand. A widespread error among untrained operators is failure to emphasize vowels sufficiently.
- Speak slowly. Give the receiving operator a chance to get your message down. This can save time and repetitions.
- Avoid extremes of pitch. A high-pitched voice cuts through interference best, but is shrill and unpleasant if too high. A lower pitch is easier on the ear, but is difficult to understand through background noises if too low.
- Be natural. Maintain a normal speaking rhythm. Group words in a natural manner. Send your message phrase for phrase instead of word for word.
- Use standard pronunciation. Talkers who use the almost standard pronunciation of a broadcast network announcer are easiest to understand.
- Speak in a moderately strong voice in order to override unavoidable background noises and to prevent dropouts.
- Keep correct distance between lips and handset. A distance of about 2 inches is correct for most handsets. If the distance is too great, speech becomes inaudible and background noises interfere. If the distance is too small, blaring and blasting result.
- Give an accurate evaluation in response to a request for a radio check. A transmission with feedback or a high level of background noise is not "loud and clear," even though the message can be understood.
- Pause momentarily after each normal phrase, and interrupt your carrier. This allows any other station with higher precedence traffic to break in.

- Adhere strictly to prescribed procedures. Up-to-date R/T procedures are found in *Radiotelephone Procedure,* ACP 125.
- Transact your business and get off the air. Excessive preliminary calls waste time.

DO NOT:

- Transmit while surrounded by others loudly discussing the next maneuver or event. It confuses the receiving stations and could be a serious security violation.
- Hold the handset button in the push-to-talk position until absolutely ready to transmit. Your carrier will block other communications on the net.
- Hold a handset in such a position that there is a possibility of having feedback from the earphone added to other background noises.
- Hold a handset loosely. A firm pressure on the push-to-talk button prevents unintentional release and consequent signal dropout.
- Tie up a circuit with test signals. Usually, 10 seconds is sufficient for testing.

PHONETIC ALPHABET

Some letters of the alphabet have similar sounds; therefore, it is easy to confine the sounds of these letters. For this reason, the standard phonetic equivalents of the letters of the alphabet are used in R/T communications. Using the phonetic alphabet saves many corrections and constant repetitions that would otherwise be necessary. Table 2-1 contains the alphabet with a list of its phonetic and spoken equivalents. The bolded portions of the spoken equivalents are the parts of the word that should be given the greatest emphasis when spoken.

When signals from naval signal books are transmitted by voice, names of flags (ALFA, BRAVO, and so on) are used since they appear in the signal books. Difficult words within the text of plain text messages may be phonetically spelled, using the phonetic alphabet, preceded by the proword I SPELL. When the operator can pronounce the word to be spelled, he or she does so before and after the spelling of the word to be identified. For example, a phrase in a plain text message might contain the words "Kisatchie Reservation." Upon reaching these two words, the operator would say, ". . .Kisatchie, I SPELL, KILO, INDIA, SIERRA, ALFA, TANGO, CHARLIE, HOTEL, INDIA, ECHO, Kisatchie, Reservation . . ." (rest of text).

Table 2-1—Phonetic Alphabet

LETTER	PHONETIC	SPOKEN AS
A	ALFA	**AL** FAH
B	BRAVO	**BRAH** VOH
C	CHARLIE	**CHAR** LEE OR **SHAR** LEE
D	DELTA	**DEL** TAH
E	ECHO	**ECK** OH
F	FOXTROT	**FOKS** TROT
G	GOLF	GOLF
H	HOTEL	HOH **TELL**
I	INDIA	**IN** DEE AH
J	JULIETT	**JEW** LEE **ETT**
K	KILO	**KEY** LOH
L	LIMA	**LEE** MAH
M	MIKE	MIKE
N	NOVEMBER	NO **VEM** BER
O	OSCAR	**OSS** CAH
P	PAPA	PAH **PAH**
Q	QUEBEC	KEY **BACK**
R	ROMEO	**ROW** ME OH
S	SIERRA	SEE **AIR** RAH
T	TANGO	**TANG** GO
U	UNIFORM	**YOU** NEE FORM or **OO** NEE FORM
V	VICTOR	**VIC** TAH
W	WHISKEY	**WISS** KEY
X	X-RAY	**ECKS** RAY
Y	YANKEE	**YANG** KEY
Z	ZULU	**ZOO** LOO

When a text is composed of pronounceable words, the words are spoken as such. When a text is encrypted, the groups are transmitted by the phonetic equivalents of the individual letters and without the proword I SPELL. For example, the encrypted group DRSRM is spoken "DELTA, ROMEO, SIERRA, ROMEO, MIKE" and is counted as one group.

PRONUNCIATION OF NUMERALS

You must use care in distinguishing numerals from similarly pronounced words. When transmitting numerals, you may use the proword FIGURES preceding such numbers. For example, the text of an R/T message contains the phrase "From Ten Companies." There is a possibility that the phrase would sound like "From Tin Companies" if spoken as it is written. An operator, therefore, could use the proword FIGURES when this phrase is reached in the text by saying "From FIGURES One Zero Companies." The operator could also use the proword I SPELL here. For example, upon reaching the same phrase in the text of the message, an operator could transmit "From Ten, I SPELL, TANGO, ECHO, NOVEMBER, Ten, Companies."

When numerals are transmitted, their correct pronunciation is as follows:

Numeral	Pronounced
0	Ze ro
1	Wun
2	Too
3	Tree
4	Fo wer
5	Fife
6	Six
7	SE ven
8	Ait
9	NIN er

The numeral 0 is always spoken as "zero," never as "oh." Decimal points are spoken as "day-see-mal."

Numbers are transmitted digit for digit except that exact multiples of thousands are spoken as such. There are, however, special cases, such as antiair warfare reporting procedures, when the normal pronunciation of numerals is prescribed and digit-for-digit transmission does not apply. For example, in the case given, the number 17 is pronounced "seventeen"; not "one seven." The following is a list of numbers and their normal R/T pronunciation:

Number	Pronounced
11	Wun Wun
55	Fife Fife
1000	Wun Tou-zand
1920	Wun Niner Too Zero
34,000	Three Fower Tou-zand
349,204	Three Fower Niner Too Zero Fower

DECIMALS, DATES, AND ABBREVIATIONS

As we mentioned earlier, the decimal point is spoken as "day-see-mal." For example, 920.4 would be spoken as "Niner Too Zero Day-see-mal Fower."

Dates are spoken digit for digit, with the months spoken in full. For example, the date 20 September is spoken as "Too Zero September."

There are some rules that you should remember concerning abbreviations in the text of an R/T message. For example, initials are spoken phonetically when used alone or with short titles. The phrase "Para A" is spoken as "Para Alfa." The initials "ACP" would be spoken as "Alfa Charlie Papa."

Personal initials are spoken phonetically, prefixed by the proword INITIALS. For example, the name "W. T. DOOR" would be spoken as "INITIALS Whiskey Tango Door."

Familiar abbreviations that are frequently used in normal speech may be transmitted in abbreviated form on R/T. For example, the word "NATO" is spoken as "NATO." The ship "USS *Canopus"* is spoken as "USS Canopus."

PUNCTUATION

When punctuation is necessary in an R/T message, the punctuation is pronounced as follows:

Punctuation	Spoken
Comma	COMMA
Period	FULL STOP or PERIOD
Parentheses	PAREN/UNPAREN or OPEN BRACKETS/CLOSE BRACKETS
Oblique Stroke	SLANT
Quotation Marks	QUOTE/UNQUOTE
Hyphen	HYPHEN
Colon	COLON
Semicolon	SEMICOLON
Dash	DASH

Roman numerals, when used, are transmitted in the same manner as the corresponding Arabic numerals and preceded by the word "ROMAN." For example, the Roman numeral III is pronounced "ROMAN Tree."

USE OF PROWORDS

Table 2-2 contains a list of authorized prowords for general use. Prowords are used to expedite message handling on circuits where R/T procedures are used. In no case may a proword or combination of prowords be substituted for the textual component of a message. Between units of different nationalities, prowords may be replaced by their equivalent prosigns where these exist. These should be spelled out using the authorized phonetic equivalents.

Table 2-2.—Radiotelephone Prowords, Equivalent Prosigns, and Operating Signals

PROWORD	EXPLANATION	EQUIVALENT TO
ACKNOWLEDGE (ACK)	An instruction to the addressee that the message must be acknowledged	ZEV
ADDRESS GROUP	The group that follows is an address group	
ALL AFTER	The portion of the message to which I have reference is all that which follows _____	AA
ALL BEFORE	The portion of the message to which I have reference is all that which precedes _____	AB
AUTHENTICATE	The station called is to reply to the challenge which follows	INT ZNB
AUTHENTICATI ON IS	The transmission authentication of this message is_____	ZNB
BREAK	I hearby indicate the separation of the text from other portions of the message	BT
BROADCAST YOUR NET	Link the two nets under your control for automatic rebroadcast	
CALL SIGN	The group that follows is a call sign	
CORRECT	You are correct, or what you have transmitted is correct	C
CORRECTION	An error has been made in this transmission. Transmission will continue with the last word correctly transmitted	EEEEEEEE
	An error has been made in this transmission (or message indicated). The correct version is _____	C
	That which follows is a corrected version in answer to your request for verification	C
DISREGARD THIS TRANSMISSION—OUT	This transmission is in error. Disregard it. This proword must not be used to cancel any message that has been completely transmitted and for which receipt or acknowledgment has been received	EEEEEEEE AR

Table 2-2.—Radiotelephone Prowords, Equivalent prosign~ and Operating Signals—Continued

PROWORD	EXPLANATION	EQUIVALENT TO
DO NOT ANSWER	Stations called are not to answer this call, receipt for this message, or otherwise to transmit in connection with this transmission. When this proword is used, the transmission must be ended with the proword OUT	F
EXECUTE	Carry out the purport of the message or signal to which this applies. To be used only with the Executive Method	IX
EXECUTE TO FOLLOW	Action on the message or signal that follows is to be carried out upon receipt of the proword EXECUTE. To be used only with the Delayed Executive Method	IX
EXEMPT	The addressees immediately following are exempted from the collective call	XMT
FIGURES	Numerals or numbers follow	
FLASH	Precedence FLASH	Z
FROM	The originator of this message is indicated by the address designator immediately following	FM
GROUPS	This message contains the number of groups indicated by the numeral following	GR
GROUP NO COUNT	The groups in this message have not been counted	GRNC
I AUTHENTICATE	The group that follows is the reply to your challenge to authenticate	ZNB
IMMEDIATE	Precedence IMMEDIATE	O
IMMEDIATE EXECUTE	Action on the message or signal following is to be carried out on receipt of the word "EXECUTE." To be used only with the Immediate Executive Method	IX
INFO	The addressees immediately following are addressed for information	INFO
I READ BACK	The following is my response to your instructions to read back	
I SAY AGAIN	I am repeating transmission or portion indicated	IMI
I SPELL	I will spell the next word phonetically	
I VERIFY	That which follows has been verified at your request and is repeated. To be used only as a reply to VERIFY	C
MESSAGE	A message that requires recording is about to follow. Transmitted immediately after the call. (This proword is not used on nets primarily employed for conveying messages. It is intended for use when messages are passed on tactical or reporting nets)	ZBO
MORE TO FOLLOW	Transmitting station has additional traffic for the receiving station	B

Table 2-2.—Radiotelephone Prowords, Equivalent Prosigns, and Operating Signals—Continued

PROWORD	EXPLANATION	EQUIVALENT TO
NET NOW	All stations are to net their radios on the unmodulated carrier wave that I am about to transmit	ZRC2
NUMBER	Station Serial Number	NR
OUT	This is the end of my transmission to you and no answer is required or expected	AR
OVER	This is the end of my transmission to you and a response is nccessary. Go ahead; transmit	K
PRIORITY	Precedence PRIORITY	P
READ BACK	Repeat this entire transmission back to me exactly as received	G
RELAY (TO)	Transmit this message to all addressees (or addressees immediately following this proword). The address component is mandatory when this proword is used	T or ZOF
ROGER	I have received your last transmission satisfactorily	R
ROUTINE	Precedence ROUTINE	R
SAY AGAIN	Repeat all of your last transmission. Followed by identification data means "Repeat _____ (portion indicated)"	IMI
SERVICE	The message that follows is a SERVICE message	SVC
SIGNALS	The groups that follow are taken from a signal book. (This proword is not used on nets primarily employed for conveying signals. It is intended for use when tactical signals are passed on nontactical nets)	
SILENCE (Repeated three or more times)	Cease transmission on this net immediately. Silence will be maintained until lifted. (When an authentication system is in force, the transmission imposing silence is to be authenticated)	HM HM HM
SILENCE LIFTED	Silence is lifted. (When an authentication system is in force, the transmission lifting silence is to be authenticated)	ZUG HM HM HM
SPEAK SLOWER	Your transmission is at too fast a speed. Reduce speed of transmission	QRS
STOP REBROADCASTI NG	Cut the automatic link between the two nets that are being rebroadcast and revert to normal working	
THIS IS	This transmission is from the station whose designator immediately follows	DE
TIME	That which immediately follows is the time or date-time group of the message	QTR
TO	The addressees immediately following are addressed for action	TO

Table 2-2.—Radiotelephone Prowords, Equivalent Prosigns, and Operating Signals—Continued

PROWORD	EXPLANATION	EQUIVALENT TO
UNKNOWN STATION	The identity of the station with whom I am attempting to establish communication is unknown	AA
VERIFY	Verify entire message (or portion indicated) with the originator and send correct version. To be used only at the discretion of or by the addressee to which the questioned message was directed	J
WAIT	I must pause for a few seconds	AS
WAIT-OUT	I must pause longer than a few seconds	AS AR
WILCO	I have received your signal, understand it, and will comply. To be used only by the addressee. Since the meaning of ROGER is included in that of WILCO, the two prowords are never used together	
WORD AFTER	The word of the message to which I have referenced is that which follows _____	WA
WORD BEFORE	The word of the message to which I have referenced is that which precedes _____	WB
WORDS TWICE	Communication is difficult. Transmit(ting) each phrase (or each code group) twice. This proword may be used as an order, request, or as information	QSZ
WRONG	Your last transmission was incorrect. The correct version is_____	ZWF

USE OF OPERATING SIGNALS

Operating signals are not designed for R/T transmission. In R/T procedures, operating information is normally conveyed in concise phrases. However, in two circumstances it is permissible to use operating signals contained in *Communication Instructions, Operating Signals,* ACP 131, instead of standard R/T phrases. These circumstances are where there are language difficulties and where practical if there is no risk of confusion.

In such instances, operating signals must be preceded by the word "PROSIGN" or "OPERATING SIGNAL." Prosigns and operating signals are transmitted using only authorized phonetic equivalents. The prosign INT is transmitted in its prosign equivalent; that is, INTERROGATIVE. The prowords I SPELL and FIGURES are not used. Examples of prosigns and operating signals are:

QRM—OPERATING SIGNAL QUEBEC ROMEO MIKE

XMT—PROSIGN X-RAY MIKE TANGO

INT ZKA—OPERATING SIGNAL INTERROGATIVE ZULU KILO ALFA

RADIOTELEPHONE SECURITY

In addition to adhering to circuit discipline, all users are responsible for observing proper security precautions on R/T nets. For example, many units at sea use classified call signs on tactical nets. If the operator does not know the operating situation, the classified call could be linked to the unclassified call sign for that ship. Such unauthorized disclosures are why BEADWINDOW procedures have been introduced into the R/T process.

BEADWINDOW

BEADWINDOW is a real-time procedure used to alert circuit operators that an unauthorized disclosure has occurred over a nonsecured circuit. BEADWINDOW also warns other operators on the net of the disclosure. This serves as an educational aid. The long-term benefits of the BEADWINDOW procedure include an increased awareness of the proper use of voice circuits throughout the fleet and better security of uncovered Navy voice communications.

BEADWINDOW procedures deal with **Essential Elements of Friendly Information (EEFIs).** EEFIs are established by operational commanders. EEFIs identify specific items of information which, if revealed and correlated with other information, would degrade the security of military operations, projects, or missions in the applicable areas. EEFIs can, therefore, vary from operation to operation or from area to area. Table 2-3 contains an EEFI key number and key word definition list.

BEADWINDOW CODE WORDS

The BEADWINDOW procedure uses the code word "BEADWINDOW" and a number combination (from the EEFI list) that is transmitted immediately to the unit disclosing an EEFI. The code word notifies the unit that it has committed the disclosure, and the number combination provides specific identity of the item disclosed. For example, when any station of the net commits a disclosure of an EEFI, net control (or any station observing the disclosure) calls the violator with

Table 2-3.—Essential Elements of Friendly Information (EEFIs)

01 Position	Friendly or enemy position, movement or intended movement: position, course, speed, altitude or destination of any air, sea, or ground element unit or force
02 Capabilities	Friendly or enemy capabilities or limitation: force composition or identity capabilities, limitations or significant casualties to special equipment, weapon systems, sensors, units, or personnel. Percentages of fuel or ammunition remaining
03 Operations	Friendly or enemy operations, intentions, progress or results: operational or logistic intentions; assault objectives; mission participants; flying programs, mission situation reports; results of friendly or enemy operations
04 Electronic Warfare (EW)	Friendly or enemy EW/EMCON intentions, progress or results: intention to employ EA; results of friendly or enemy EA; objectives of EA; results of friendly or enemy EP; results of ESM; present or intended EMCON policy; equipment affected by EMCON policy
05 Personnel	Friendly or enemy key personnel: movement or identity of friendly or enemy flag officers: distinguished visitors; unit commanders; movements of key maintenance personnel indicating equipment limitations
06 COMSEC	Friendly or enemy COMSEC locations: linkage of codes or code words with plain language; compromise of changing frequencies or linkage with line numbers, circuit designators linkage of changing call signs with previous call signs or units; compromise of encrypted/classified call signs; incorrect authentication procedure
07 Wrong Circuit	Inappropriate transmission: information requested, transmitted or about to be transmitted which should not be passed on the subject circuit because it either requires greater security protection or is not appropriate to the purpose for which the circuit is provided
08	For NATO assignment, as required
09	For NATO assignment, as required
10	For NATO assignment, as required
11-29	Reserved for CINCUSNAVEUR
30-49	Reserved for CINCLANTFLT
50-69	Reserved for CINCPACFLT

a normal call-up. The calling station then says the word "BEADWINDOW" followed by the number of the EEFI the violator disclosed.

The only authorized reply to the BEADWINDOW message is "ROGER-OUT." This method allows the reported unit to take immediate action to correct the insecure practice. In this particular situation, if the call sign of the net control is "Control" and the call sign of the violator is USS *Frances Scott Key,* Control's report would be:

"Key, THIS IS Control, BEADWINDOW Three, OVER."

The violator would reply:

"Control, THIS IS Key, ROGER, OUT."

The EEFI list should be posted in clear sight of the operator at all nonsecure voice positions for quick reference. You should remember that procedural violations are not security violations; therefore, they don't fall in the BEADWINDOW category.

IMPORTANCE OF RADIOTELEPHONE VOICE PROCEDURES

Poor voice communications can create confusion, reduce reliability and speed, and nullify security precautions. Poor procedures can ultimately have an adverse effect on the mission of a ship.

A commanding officer, regardless of the mission of the ship, has only one real-time means of communicating with his commander and other units of a force—radiotelephone. Your ship maybe required to guard (monitor) 10 or more voice circuits, each having a specific purpose and specific procedures. Few of these circuits are operated from communications spaces except on small ships, such as submarines or destroyers. On larger ships, the circuits are handled from the bridge and the combat information center (CIC).

As an operator, you are responsible for providing reliable transmitter and receiver services to these remote operating positions. This entails establishing communications on a net or circuit before making that net or circuit available to the remote operators. If you do not know the various nets that are guarded by your ship and the purpose of these nets, the overall communications of the ship can be degraded. This could impede the progress of the entire operation.

Modern, high-speed naval operations make the elimination of confused R/T operations an absolute necessity. For example, a hunter-killer force searching for an enemy submarine is not permitted the luxury of a 5- or 10-minute delay in executing a screening signal. An unnecessary delay such as this could defeat the purpose (speed) of the officer in tactical command (OTC) when using R/T. A 1-minute delay by an aircraft carrier pilot in executing a vectoring signal because he did not understand the message could easily result in the pilot's death.

During shakedown operations, a submarine could risk collision with its escort vessel during emergency surfacing procedures if voice communications are not clearly understood.

When possible, you must use only standard phraseology, authorized prowords, and brevity code words. Standard procedures enhance reliability and clarity. Moreover, variations from standard circuit procedures provide an ideal situation for enemy imitative deception.

BASIC RADIOTELEPHONE MESSAGE FORMAT

Radiotelephone uses a 16-line message format (table 2-4) that is comparable to formats in teleprinter communications. Radiotelephone messages also have the same three military message forms: plaindress, abbreviated plaindress, and codress.

By far, the most common message form in R/T traffic is the abbreviated plaindress. In fact, the abbreviated plaindress message is sometimes so abbreviated that it closely resembles the basic message format. The three major message parts-heading, text, and ending—are there, however. Each of these major parts is reduced to components and elements.

All format lines do not necessarily appear in every message. When a line is used, it must be placed in the message in the order shown in table 2-4. An abbreviated plaindress message may omit any or all of the following: precedence, date, date-time group (DTG), and/or group count. A codress message is one in which the entire address is encrypted within the text. The heading of a codress message contains only information necessary to enable communications personnel to handle it properly.

Notice that prowords, not prosigns, are used in voice communications. Because prowords are spoken, it is important that you, as the operator, be completely familiar with them. Refer to table 2-2 for a list of many of the commonly used prowords, their explanations, and their equivalent prosigns. Throughout this chapter, prowords are shown in all capital letters.

Table 2-4.—Radiotelephone Message Format

PARTS/ COMPONENT S		ELEMENTS	FORM AT LINE	CONTENTS
HEADING	Procedure	a. Call	1	Not used
		b. Message follows	2 & 3	Stations called—Proword EXEMPT, exempted calls
		c. Transmission Identification		Proword THIS IS—station calling
				Proword MESSAGE
		d. Transmission Instructions		Proword NUMBER and station serial number
			4	Prowords RELAY TO; READ BACK; DO NOT ANSWER; WORDS TWICE; Operating signals; Address Groups; Call Signs; Plain Language designators
	Preamble	a. Precedence; date-time group; message instructions	5	Precedence designation; Proword TIME: date and time expressed in digits, and zone suffix followed by month indicated by the first three letters and, if required by national authorities, the year indicated by the last two digits; operating signals and proword EXECUTE TO FOLLOW
	Address	a. Originator's Sign; Originator	6	Proword FROM. Originator's address designator
		b. Action Addressee Sign	7	Proword TO. Action addressee designator
		c. Information Addressee Sign; Information Addressee	8	Proword INFO. Information addressees designators
		d. Exempted Addressee Sign; Exempted Addressee	9	Proword EXEMPT. Exempted addressee designators
	Prefix	a. Accounting Information, group count	10	Accounting symbol; group count; Proword GROUPS (GROUP NO COUNT)
SEPARATION			11	Proword BREAK
TEXT	Text	a. Subject Matter	12	CLEAR, UNCLASSIFIED, proword SERVICE, and/or internal instructions as appropriate; thoughts or ideas as expressed by the originator
SEPARATION			13	Proword BREAK
ENDING	Procedure	a. Time Group	14	Proword TIME. Hours and minutes expressed in digits and zone suffix, when appropriate
		b. Final Instructions	15	Prowords WAIT, CORRECTION, AUTHENTICATION IS, MORE TO FOLLOW, Station designators.
		c. Ending Sign	16	Prowords OVER, OUT

In the following paragraphs, we will discuss the format lines used in the R/T message format. Refer to table 2-4.

FORMAT LINES 1, 2, 3, AND 4

Format line 1 is not used in R/T procedures. Format lines 2 and 3 contain the call sign, the proword MESSAGE, and the transmission identification.

The call may take one of the following forms:

Full Call

"Kamehameha (station called),

THIS IS

Vallejo" (station calling)

Abbreviated Call

"THIS IS

Vallejo" (station calling).

Normally, a full call is used when first establishing a net and when reporting into a previously established net. A full call is also used in the transmission instructions and address components when a message is required to be relayed to a station on a different net.

Once communications are established and no confusion will result, an abbreviated call may be used. To further expedite voice communications, the receiving station may omit the proword THIS IS when the station is responding to a call and communications are good. Additionally, the call may be omitted entirely when two stations are in continuous communication or the net is not shared by a third station.

When a collective call sign is used and some of the addressees are to be exempted, you do so in the call by using the proword EXEMPT, followed by the call sign(s) of the station(s) exempted. For example:

"Edison (collective call)

EXEMPT

Tecumseh (station exempted),

THIS IS

Vallejo" (station calling).

Notice that only one station is exempted in this call-up. If there had been more than one station, each station would have been spoken before the proword THIS IS.

After the call, transmit the proword MESSAGE if you wish to indicate that a message you are about to transmit requires recording. For example:

"Vallejo (station called),

THIS IS

Kamehameha (station calling)

MESSAGE" (message is to follow).

The transmission identification is normally a station serial number used mostly in teleprinter procedures. When used in voice communications, the transmission identification is the last element of format lines 2 and 3, consisting of the station serial number preceded by the proword NUMBER.

Format line 4 contains the transmission instructions, which may consist of the prowords RELAY TO, WORDS TWICE, DO NOT ANSWER, or READ BACK. The use of these prowords is explained later.

FORMAT LINE 5

Format line 5 contains the precedence, DTG, and any necessary message instructions. The precedence is the first element of format line 5. In the case of a dual-precedence message, the higher precedence is transmitted first; for example, "PRIORITY ROUTINE." The DTG is preceded by the proword TIME. An example of this format line is as follows:

"Vallejo, THIS IS Polk, RELAY TO Key, PRIORITY, TIME, Tree Zero Wun Fower Fower Fife Zulu."

Message instructions are not normally required in R/T messages. When included, they consist of short and concise instructions that indicate the status of the message. Message instructions remain with the message until the message reaches its destined station. For example, if the message is a suspected duplicate, the phrase "This Message Is A Suspected Duplicate" immediately follows the DTG.

FORMAT LINES 6, 7, 8, AND 9

Format lines 6, 7, 8, and 9 form the address of the message and are recognized by the prowords FROM, TO, INFO, and EXEMPT, respectively. When the originator and the addressee are in direct communication, the call may serve as the address. Table 2-5 is an example of an R/T transmission showing elements of the heading components (format lines 2 through 9).

Table 2-5.—R/T Message Showing All Possible Elements of the Address Components.

Transmission	
F/L 2&3	LINCOLN (Collective Call)
	THIS IS
	POLK
	MESSAGE
F/L 5	PRIORITY
	TIME
	THREE ZERO ONE FIVE ONE
	ZERO ZULU
F/L 6	FROM
	POLK
F/L 7	TO
	LINCOLN
F/L 8	INFO
	KEY
F/L 9	EXEMPT
	EDISON (Exempted addressee from Collective Call)

FORMAT LINE 10

Format line 10 is identified by the proword GROUPS, followed by the number of groups, or "GROUP NO COUNT." This line may contain an accounting symbol in addition to the group designation. Accounting symbols are seldom used on R/T circuits. However, they may appear on messages received for relay from circuits using other procedures. Accounting symbols are a combination of letters used to indicate the agency, service, or activity that assumes financial responsibility for the message.

Since R/T messages are usually short, a group count is seldom used. However, if a group count is sent, the number of groups is preceded by the proword GROUPS and appears in the message prefix. When a message is transmitted before the group count is determined, the proword GROUP NO COUNT is used in lieu of the group count. The actual group count may then be transmitted in the final instructions and be inserted in the message prefix by the receiving operator. The proword GROUP NO COUNT is included in messages bearing an accounting symbol when groups are not counted.

FORMAT LINES 11 THROUGH 16

Format line 11 contains the proword BREAK. This line separates the heading from the text. The use of this proword is not required except where confusion may be possible between the heading and text.

Format line 12 is the text of the message and expresses the idea of the originator. The primary difference between R/T text and other types of communication is that R/T text must be spoken. Therefore, it is important that new operators thoroughly familiarize themselves with the proper phrases and prowords that are commonly used in communications texts.

Format line 13 contains the proword BREAK. This line separates the text from the ending. Like format line 11, this proword should be used when confusion may occur between the text and the ending.

Format line 14 is used only in abbreviated plaindress messages when a time group is transmitted here. When used, it takes the place of a DTG in format line 5. For example, a DTG may not be determined prior to transmission. In such cases, it may be omitted in format line 5 and be sent as a time group in format line 14. When used, format line 14 consists of the proword TIME, followed by the time group plus the zone suffix. For example, you are in time zone B and you are sending a time group of 310850 in format line 14. You would transmit the time group as:

"TIME Three One Zero Eight Five Zero Bravo."

Format line 15 contains any final instructions. When used, this line may contain prowords (such as WAIT, CORRECTION, MORE TO FOLLOW, AUTHENTICATION IS), operating signals, address groups, call signs, and plain language designators.

Format line 16 is identified by the proword OVER or OUT. Every transmission ends with either OVER or OUT. However, the proword OVER may be omitted when two stations are in continuous communication with each other on a circuit not shared with a third station. In transmissions where the proword DO NOT ANSWER is used, the transmissions must end with the Proword OUT.

RADIOTELEPHONE CALL SIGNS

Call signs used in radiotelephone are commonly known as voice call signs. They consist of spoken words, which can be transmitted and understood more rapidly and more effectively than actual names of ships and afloat commands, or phonetic equivalents of international radio call signs. Under certain circumstances, however, the phonetically spelled international call sign is used in R/T for station identification. At other times, a ship's name serves as the call sign.

R/T call signs may be assigned by an operation order (OPORD), a tactical communication plan (COMMPLAN), or permanently by commonly held communications publications. R/T call signs may be either permanent or temporary, and they may be internationally usable or locally issued. In any event, call signs are used to identify the station and to establish communications. A station's call sign can be any of the following:

- The name of the ship or aircraft tail number;
- A voice call sign listed in *Joint Voice Call Sign Book,* JANAP 119;
- An allied voice call sign listed in *Tactical Call Sign Book (U),* ACP 110; and/or
- A call sign for ships listed in *Call Sign Book for Ships,* ACP 113.

Voice Communications, NTP 5, lists publications that contain encrypted and daily changing call signs.

A ship must use its call sign when first establishing a net or when reporting into a previously established net. After this initial contact, an abbreviated form of communications may be used.

If call sign encryption is in effect and a ship or unit name appears in the text, the name should be replaced by the encrypted call sign or address group of the ship or unit. When used in this manner, the call sign or address group may be preceded by the proword CALL SIGN or ADDRESS GROUP, as applicable.

ACP 113 CALL SIGNS

ACP 113 lists the international call signs and hull numbers for ships under military control. The call signs in this publication are unclassified. International call signs are used for all nonmilitary communications and military communications using unencrypted call signs.

JANAP 119 VOICE CALL SIGNS

Voice call signs contained in JANAP 119 are pronounceable words. They are for tactical use and are designed to facilitate speed on tactical radio circuits. Secure voice call signs can be achieved only by a conscientiously applied system for changing call signs on a frequent and periodic basis.

CALL SIGNS ON LOCAL HARBOR CIRCUITS

JANAP 119 does not assign voice call signs to administrative shore activities. Consequently, a ship cannot use a tactical call on administrative ship-shore circuits. When operating on ship-shore R/T circuits, a ship may use its international call sign. Operators must speak the call sign phonetically. For example, you would speak the international call sign NOKB as "November Oscar Kilo Bravo." The procedure described in the next paragraph may also be used.

In U.S. ports and U.S.-controlled ports overseas, the name of the ship serves as the voice call sign. As a rule, the USS prefix, hull designation and number, or the first name or initials of the ship need not be included in the voice call unless essential for clarity. This procedure also applies to shore activities on administrative nets. Each activity may use its administrative title in an abbreviated form, consistent with clarity. For example, Mobile Technical Unit 2 may have a voice call of MOTU on an administrative circuit.

Port authorities that control local harbor voice circuits are identified by the word "CONTROL." For example, let's say that the Key is entering port in New London, Conn. Key's initial call to New London Control to check into the local harbor net would be:

"Control, THIS IS Key, OVER."

If *Key* were to call Fuel Control, its call would be:

"Fuel Control, THIS IS Key, OVER."

You must remember that the simplified type of call is authorized only in U.S. ports or U. S.-controlled ports. If a ship is in a port not under U.S. control, it must conform to the international practice of using phoneticized international call signs on R/T circuits.

RADIOTELEPHONE CIRCUITS

Voice communications requirements are grouped into two basic categories: operational or tactical, and administrative.

OPERATIONAL OR TACTICAL CIRCUITS

Most voice circuits used at sea are operational or tactical nets; some circuits, however, are often used to pass administrative traffic. These circuits are subcategorized into two distinct types: short and long range.

Short-range operational communications normally use the UHF frequency spectrum (225 to 400 MHz) and low-power, line-of-sight equipment. Because of these frequency and equipment characteristics, the maximum effective range is usually 20 to 25 miles. This limited UHF range offers no security, and transmissions are always subject to enemy interception. However, since these transmissions are limited somewhat to the local geographic area, interception by an enemy would be difficult. On the other hand, the range of UHF communications may be extended through the proper use of relay procedures.

More and more, our modern and high-speed ships must report to OTCs from longer distances than the older ships they replaced. Long-range frequencies in the medium- and high-frequency spectrum (2 to 32 MHz) are, therefore, used. From your study of module 4, you will remember that the propagation characteristics of these frequencies make them desirable for long-range communications. To further increase the range capabilities of long-range communications, we use single-sideband (SSB) methods.

ADMINISTRATIVE CIRCUITS

Administrative circuits are normally used only in port and may include both short- and long-range communications. Voice circuits that are neither operational nor tactical are included in the administrative category. Seldom is there such a circuit in at-sea communication plans.

Harbor common circuits and tug control nets are two examples of administrative nets. Naturally, these nets assume an operational function during situations requiring emergency procedures, such as natural disasters and civil uprisings. Circuit requirements vary from port to port, as established by the senior officer present afloat (SOPA). Both the UHF and MF/HF circuits may be used for administrative nets.

TYPES OF NETS

There are two types of R/T nets: directed and free. The type of net to be used is determined by the operational situation. Regardless of the type of net used, a Net Control Station (NECOS) is assigned to monitor the circuit or circuits and enforce circuit discipline.

NECOS is the senior net member or designated authority. The NECOS is responsible for implementing operational procedures and enforcing discipline and security on the net. Enforcement of circuit discipline, however, is not the only reason for having a NECOS. Sometimes there are so many stations sharing a common circuit that a NECOS is necessary to facilitate the handling and passing of R/T traffic.

Directed Net

On a directed net, stations must obtain permission from the NECOS before communicating with other stations on the net. The exception to this rule is when a station has FLASH traffic to send. Also, transmissions on the directed net may be accomplished with a predetermined schedule.

Free Net

On the free net, member stations don't need NECOS permission to transmit. Net members must ensure that the net is not in use before initiating a call-up. A free net, however, does not relieve the NECOS of the responsibility for enforcing operational procedures and maintaining proper circuit discipline.

Both free and directed nets normally use collective call signs. Figure 2-1 diagrams an R/T net that consists of the following stations: USS Key, USS *Mariano G. Vallejo,* USS *James K. Polk,* USS *Kamehameha,* and USS *Tecumseh.* In this example, we will assume that the NECOS is *Key.* Notice that the collective call sign for the entire net is Poseidon.

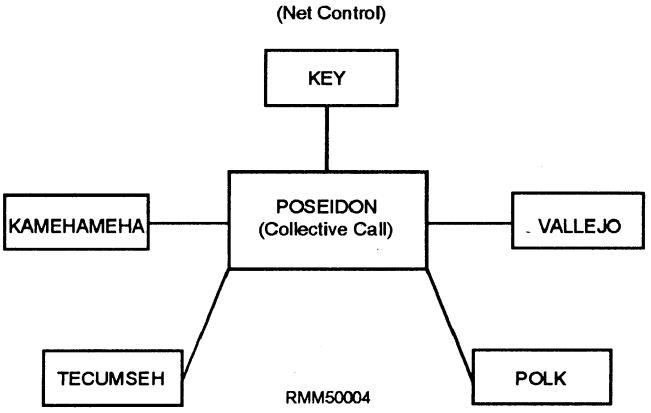

Figure 2-1.—Radiotelephone net.

OPENING THE NET

The responsibility for opening the net for the first time or reopening the net after it has been temporarily secured belongs to *Key*. To accomplish this on a free net, *Key* would transmit:

"Poseidon, THIS IS Key, OVER."

After the transmission, all stations answer in alphabetical order:

"Key, THIS IS Kamehameha, OVER,"

"Key, THIS IS Polk, OVER," (and so on until all stations have responded).

After all stations on the net have answered, Key then sends:

"Poseidon, THIS IS Key, OUT."

This last message from *Key* informs all stations that their transmissions were heard and there is no traffic for them at the time.

If a station does not reply to the collective call within 5 seconds, the next station answers in proper sequence. Barring any difficulties the station may have, the delinquent station answers last. If the delinquent station is having difficulty that prevents an answer to the call, it reports in to the net as soon as possible with the transmission:

"Key, THIS IS (name of station).

Reporting In To Net, OVER."

At this time on the free net, and following a preliminary call, the stations concerned would start transmitting traffic to each other. For example, if *Vallejo* has traffic for *Kamehameha,* it would let *Kamehameha* know this with the call:

"Kamehameha, THIS IS Vallejo, OVER."

Kamehameha would acknowledge with:

"Vallejo, THIS IS Kamehameha, OVER."

Vallejo would then send its traffic.

On the directed net, when all communications over the net are controlled by the NECOS, *Key* would call the member stations and announce that the net is directed. In this initial transmission, *Key* would request information on the status of any outstanding messages. For example:

"Poseidon, THIS IS Key, This Is A Directed Net, Of What Precedence And For Whom Are Your Messages, OVER."

Each subordinate station then answers in alphabetical order, indicating its traffic on hand. For example:

"Key, THIS IS Polk, I Have One IMMEDIATE And One PRIORITY For You, OVER."

"Key, THIS IS Vallejo, No Traffic, OVER." (Other stations respond.)

After all stations have checked into the net, *Key* would ROGER for the transmissions and commence to clear traffic in the order of priority. For example:

"Poseidon, THIS IS Key, ROGER, Polk Send Your IMMEDIATE, OVER."

After *Polk* has sent its transmission and obtained a receipt, net control then gives permission to transmit to the station with the next higher precedence traffic.

After the initial traffic is cleared, stations having messages to transmit to other stations on the net must first obtain permission from net control. For example:

"Key, THIS IS Tecumseh, I Have One ROUTINE For Polk, OVER."

Net control then answers:

"THIS IS Key, Send Your Message, OVER."

As you can see from our examples, circuit discipline is essential. Regardless of whether a single ship is entering port or several ships are engaged in a major fleet exercise, voice communications are required. The number of necessary circuits and nets increases with the complexity of the task and the number of units participating.

Whether the net is free or directed, the Net Control Station has the primary responsibility for expediting message traffic. Each station is responsible for assisting net control in the proper passing of traffic. Adherence to proper operating procedures and communications standards is essential in keeping a net free of backlogs and tie-ups.

ESTABLISHING COMMUNICATIONS

We have already discussed the procedure for calling and answering on free and directed nets. There will also be times when you will need to establish communications with a ship or station on a temporary basis to pass message traffic. This consists of nothing more than a simple call-up to initiate contact and to determine whether communications conditions are good. For example, if the USS *Ohio* wants to contact

the USS *Alabama* on a commonly guarded frequency, *Ohio's* initial call would be:

"Alabama, THIS IS Ohio, OVER."

Upon hearing the initial call, *Alabama* would reply:

"Ohio, THIS IS Alabama, OVER."

At this point, *Ohio* would initiate another call-up and indicate that it has traffic to pass to *Alabama.*

To use the circuit more efficiently, the operator should observe the following procedures:

Write down all messages or their substance prior to transmission, including those that must be delivered by the receiving operator to another person and those that are preceded by the proword MESSAGE.

Listen to make sure that the circuit is clear before initiating a transmission.

Speak in a clear, natural voice and pause after each natural phrase.

If technically practical, during the transmission of a message, the operator should pause after each natural phrase and momentarily interrupt his transmission (carrier). This will allow another station to break in if necessary.

Sometimes the operator must initiate test signals for the adjustment of either a transmitter or a receiver. Such signals should not exceed 10 seconds and should be composed of spoken numerals (1, 2, 3, and so on), followed by the call sign of the station transmitting the signals.

SEQUENCE OF CALL SIGNS

Call signs or address groups in message headings should be arranged alphabetically in the order in which they are to be transmitted, whether plain or encrypted. For this purpose, the slant sign (/) and numerals 1 through 0 are considered the 27th through the 37th letters of the alphabet. When abbreviated call signs are used on a net, the sequence of answering a collective call should be the same as if full call signs were used. This will prevent confusion when these call signs are changed from full to abbreviated.

SIGNAL STRENGTH AND READABILITY

A station is presumed to have good signal strength and readability unless the operator is notified otherwise. Queries concerning signal strength and readability should not be exchanged unless one station cannot clearly hear another station. The proword RADIO CHECK is the standard phrase used in a call-up that questions signal strength and readability. For example, let's assume that USS *Alabama* initiates a call to USS *Ohio* and wishes to know the status of communications conditions. *Alabama's* initial call would be:

"Ohio, THIS IS Alabama, RADIO CHECK, OVER."

Upon hearing this transmission satisfactorily and determining that communications conditions are clear, *Ohio* would then answer:

"Alabama, THIS IS Ohio, ROGER, OVER."

The omission of comment on signal strength and readability is understood by *Alabama* to mean that the reception is loud and clear. If any adverse conditions existed that were impeding *Ohio's* ability to maintain satisfactory communications, *Ohio* would have used one of the phrases (considered prowords) in table 2-6.

Table 2-6.—Prowords Concerning Signal Strength and Readability

(1) **General:**	
RADIO CHECK	What is my signal strength and readability; that is, how do you hear me?
ROGER	I have received your last transmission satisfactorily. The omission of comment on signal strength and readability is understood to mean that reception is loud and clear. If reception is other than loud and clear, it must be described with the prowords in the below paragraphs
NOTHING HEARD	To be used when no reply is received from a called station
(2) **Report of Signal Strength:**	
LOUD	Your signal is very strong
GOOD	Your signal strength is good
WEAK	Your signal strength is weak
VERY WEAK	Your signal strength is very weak
FADING	At times, your signal strength fades to such an extent that continuous reception cannot be relied upon
(3) **Report of Readability:**	
CLEAR	Excellent quality
READABLE	Quality is satisfactory
UNREADABLE	The quality of your transmission is so bad that I cannot read you
DISTORTED	Having trouble reading you because your signal is distorted
WITH INTERFERENCE	Having trouble reading you due to interference
INTERMITTENT	Having trouble reading you because your signal is intermittent

For example, if *Ohio* did not consider the transmission satisfactory, *Ohio* might reply:

"Alabama, THIS IS Ohio, WEAK And DISTORTED, OVER."

A station that wishes to inform another station of signal strength and readability does so by means of a short report of actual reception. A short report maybe "Weak but readable" or "Weak with interference." Such reports as "Five by" or "Four by four" are not authorized and are not indicative of signal strength and quality of reception.

COMMUNICATIONS CONDITIONS

Situations exist where atmospheric conditions and interference do not present problems to successful communications. During good conditions, message parts need only be transmitted once, and, depending upon the operational situation, preliminary calls are sometimes optional.

At other times, conditions are anything but ideal and can present problems to even an experienced operator. Normal operating procedure requires an operator to transmit all call signs twice when communications conditions are bad. During bad conditions, phrases, words, or groups to be transmitted twice are indicated by the use of the proword WORDS TWICE. Reception may be verified by use of the proword READ BACK. For example, if bad communications conditions exist and *Tecumseh* has a message for *Kamehameha* that reads "Moor Starboard Side Tender," the transmission would be:

"Kamehameha, Kamehameha, THIS IS, Tecumseh, Tecumseh, WORDS TWICE, WORDS TWICE, Moor Starboard Side Tender Moor Starboard Side Tender, OVER."

Upon receipt of the message, *Kamehameha* would ROGER for it. To ensure reception during bad communications conditions, *Tecumseh* could have ended the above transmission with the proword READ BACK, sent twice. This would require *Kamehameha* to read back the message verbatim in WORDS TWICE form, thus ensuring that the message was properly received.

Another method of using the READ BACK procedure is to do so without using WORDS TWICE. If *Tecumseh* wanted *Kamehameha* to read back the message to ensure reception but did not want to use the WORDS TWICE procedure, *Tecumseh's* transmission would be:

"Kamehameha, THIS IS Tecumseh, READ BACK Text, BREAK, Moor Starboard Side Tender, OVER."

Kamehameha would then answer:

"Tecumseh, THIS IS Kamehameha, I READ BACK Text, Moor Starboard Side Tender, OVER."

Satisfied that *Kamehameha* has properly received the message, *Tecumseh* would then send:

"Kamehameha, THIS IS Tecumseh, That Is Correct, OUT."

If *Kamehameha* repeated back the message incorrectly, *Tecumseh* would have used the proword WRONG, followed by the correct version. *Kamehameha* would then repeat back the necessary portions until the entire message was correctly received.

When using the WORDS TWICE or READ BACK procedure, you should remember several rules. First, the prowords THIS IS and OVER are not repeated twice when using the WORDS TWICE procedure. These prowords are not spoken twice in the original transmission nor in the repeat back version. Second, the proword ROGER is not necessary to indicate receipt of the message in the READ BACK procedure. If the message is correct in its repeated back version, you would use the phrase "THAT IS CORRECT, OUT."

In a collective call where only some of the stations represented are to read back, those stations should be specified by transmitting their appropriate call signs preceding the proword READ BACK. When the order to read back is given, only those stations directed to do so will read back. The remaining stations called will keep silent unless directed by the calling station to receipt. When not preceded by identifying call signs, the proword READ BACK means that all stations are to read back if the call is a collective one.

CORRECTIONS

When a transmitting operator makes an error, the operator uses the proword CORRECTION to correct it. The operator then repeats the last word, group, proword, or phrase correctly sent, corrects the error, and proceeds with the message. For example, let's assume that *Tecumseh* made a mistake in the message to *Kamehameha. The* method *Tecumseh* uses to correct that mistake is:

"Kamehameha, THIS IS Tecumseh, Moor Outboard Side, CORRECTION, Moor Starboard Side Tender, OVER."

If an error in a message is not discovered until the operator is some distance beyond the error, the operator may make the correction at the end of the message. Let's assume that *Key* is communicating with *Polk.* During *Key's* transmission, *Key* makes a mistake in the time group but the mistake is not discovered until near the end of the transmission. The procedure *Key* would make to correct the mistake is:

"Polk, THIS IS Key, TIME Zero Eight Two Four Zulu, BREAK, Request Status Deep Dive, BREAK, CORRECTION, TIME Zero Eight Two Five Zulu, OVER."

REPETITIONS

When words are missed or cannot be determined, stations may request repetitions before receipting for the message. The prowords most often used for obtaining repetitions are SAY AGAIN, ALL BEFORE, ALL AFTER, WORD BEFORE, WORD AFTER, and TO. For example, in the previous message from *Key* to *Polk,* assume that *Polk* missed the entire message after the word "Request." *Polk's* request for a repetition for that portion of the message would be:

"Key, THIS IS Polk, SAY AGAIN ALL AFTER Request, OVER."

Key would then reply:

"THIS IS Key, I SAY AGAIN ALL AFTER Request—Status Deep Dive, BREAK, OVER."

Upon satisfactory receipt, *Polk* would send:

"THIS IS Polk, ROGER, OUT."

This same procedure applies for the proword ALL BEFORE.

The repetition procedure is also used when a station requests that a particular word be repeated. This is done by using either of the prowords WORD AFTER or WORD BEFORE. For example:

"Key, THIS IS Polk, SAY AGAIN WORD AFTER Status, OVER."

Key then replies:

"THIS IS Key, I SAY AGAIN WORD AFTER Status-Deep, OVER."

The WORD BEFORE procedure would be accomplished in the same way by simply substituting the prowords.

The use of the proword TO is as follows:

"Key, THIS IS Polk, SAY AGAIN Request TO Dive, OVER."

Key would then reply:

"THIS IS Key, I SAY AGAIN Request TO Dive—Request Status Deep Dive, OVER."

Upon satisfactory receipt, *Polk* would reply:

"THIS IS Polk, ROGER, OUT."

An important rule to remember is that when you request repetitions in the heading of an R/T message containing FROM, TO, INFO, or EXEMPT addressees, the prowords are the key to the repetition procedures. Repetitions may be requested for all of that portion of the heading preceding or following a proword or that portion between any two prowords. For example, *Key* sends the following message to *Polk:*

"Polk, THIS IS Key, MESSAGE, PRIORITY, TIME, Zero Eight Zero Nine Three Zero Zulu, FROM Key, TO Polk, INFO Tecumseh, BREAK, Proceed Naval Underwater Sound Laboratories, Rendezvous SAQAD, I SPELL, Sierra, Alfa, Quebec, Alfa, Delta, SAQAD, Representative, BREAK, OVER."

Polk misses *the* portion of the message before the address and sends:

"Key, THIS IS Polk, SAY AGAIN ALL BEFORE FROM, OVER."

Key then sends:

"Polk, THIS IS Key, I SAY AGAIN ALL BEFORE FROM—Polk, THIS IS Key, MESSAGE, PRIORITY, TIME, Zero Eight Zero Nine Three Zero Zulu, OVER."

Upon understanding the missing portion, *Polk* sends:

"Key, THIS IS Polk, ROGER, OUT."

This same procedure can be applied to all repetition prowords. An important point for you to remember is that requests for repetition must include those portions of the heading before, after, or between the applicable prowords.

CANCELING MESSAGES

Before the ending proword OVER or OUT is sent, a station can cancel a message transmission by using the proword DISREGARD THIS TRANSMISSION, OUT. For example, if *Key* should realize, while sending a message, that the message is being sent in error, *Key* would cancel the transmission as follows:

". . . Proceed Underwater Sound Laboratories, DISREGARD THIS TRANSMISSION, OUT."

After a message has been completely transmitted, it can be canceled only by another message. For example:

"Polk, THIS IS Key, Cancel My Zero Eight Zero Nine Three Zero Zulu, TIME Zero Nine Five Zero Zulu, OVER."

Polk transmits:

"Key, THIS IS Polk, ROGER, OUT."

RECEIPT OF A MESSAGE

No message is considered delivered on an R/T circuit until the transmitting station receives a receipt. A receipt is effected by the use of the proword ROGER. The receiving station can transmit a receipt after each message or after a string of messages if there is more than one message to be receipted for.

In a collective net, the transmitting station may determine that speed of handling should be the primary consideration. In this case, one station in the net maybe directed to receipt for the message or messages and no other station may answer until instructed to do so. This, however, does not prohibit any station in the net from requesting repetition.

ACKNOWLEDGMENT OF R/T MESSAGES

You should not confuse an acknowledgment with a reply or receipt. An acknowledgment is a reply from an addressee indicating that a certain message was received, understood, and can be complied with. A receipt means only that the message was received satisfactorily. Only the commanding officer or his or her authorized representative can authorize communications personnel to send an acknowledgment.

A request for acknowledgment is accomplished by use of the word "acknowledge" (not a proword) as the final word of the text. The reply is the proword WILCO. If the commanding officer can acknowledge at once, the communications operator may receipt for the message with WILCO because the meaning of ROGER is contained in WILCO. If the acknowledgment cannot be returned immediately, the communications operator receipts for the message with ROGER, and replies with WILCO later. The return transmission to a request for an acknowledgment is either ROGER or WILCO; never both. For example, *Polk* receives the following transmission from *Key:*

"Polk, THIS IS Key, Request Special Communications Training, Acknowledge, OVER."

The commanding officer wishes to consider the request before acknowledging; the operator sends:

"Key, THIS IS Polk, ROGER, OUT."

After consideration, the commanding officer of *Polk* understands and can comply with the message. The operator then transmits:

"Key, THIS IS Polk, WILCO, OUT."

VERIFICATION OF R/T MESSAGES

When a receiving station requests verification of an R/T message, the originating station verifies the message with the originating person, checks the cryptography (if the message is encrypted), and sends the correct version. For example:

"Key, THIS IS Polk, VERIFY your Zero Eight Zero Nine Three Zero Zulu—SAY AGAIN FROM TO INFO, OVER."

Key then transmits:

"THIS IS Key, ROGER, OUT."

After checking with the originating officer, *Key* determines that the portion to be verified is correct as transmitted previously and sends:

"Polk, THIS IS Key, I VERIFY My Zero Eight Zero Nine Three Zero Zulu, I SAY AGAIN, FROM TO INFO—FROM Key, TO Polk, INFO, OVER."

Polk receipts for the transmission:

"THIS IS Polk, ROGER, OUT."

BREAK-IN PROCEDURES

A station having a message of higher precedence than the transmission in progress may break in and suspend that transmission in the following manner:

FLASH message—The station should break in at once and transmit the message.

IMMEDIATE message—The station may break in at once and pass the message. The station may make a preliminary call before transmitting the message, if necessary. On a directed net, the station must obtain control approval before transmitting the message.

PRIORITY message—The station should use the same procedure as for IMMEDIATE, except that only long ROUTINE messages should be interrupted.

You should be aware that the break-in procedure is not to be used during the transmission of a tactical message except to report an enemy contact. The precedence of the message spoken three times means to cease transmissions immediately. Silence must be maintained until the station breaking in has passed the message. In the following example, assume that *Tecumseh* is transmitting a message to *Kamehameha* on a free net and *Key* has a FLASH message for *Polk. Key* breaks in with the following transmission:

"FLASH, FLASH, FLASH, POLK, THIS IS Key, FLASH, OVER."

Polk replies:

"THIS IS Polk, ROGER, OVER."

Key then proceeds with the FLASH traffic and obtains a proper ROGER, thus freeing the net for further transmissions. After hearing "ROGER," *Kamehameha* recontacts *Tecumseh* for the remainder of the traffic that was being sent before the break-in:

"Tecumseh, THIS IS Kamehameha, ALL AFTER . . . . "

On a directed net, the station wishing to break in would first obtain permission from net control. For example, referring to figure 2-1, assume that *Vallejo* is transmitting a message to *Kamehameha* and *Polk* has FLASH traffic for *Tecumseh. Polk* notifies *Key* (net control):

"FLASH, FLASH, FLASH, Key, THIS IS Polk." FLASH For Tecumseh, OVER."

Key then answers:

"Polk, THIS IS Key, Send Your FLASH, OVER."

Upon hearing the authorization, *Tecumseh* transmits:

"THIS IS Tecumseh, OVER."

Polk proceeds:

"Tecumseh, THIS IS Polk, FLASH (sends message), OVER."

The preceding transmission would conclude after *Polk* had received a proper ROGER for the FLASH traffic. The two stations that were broken *(Vallejo* and *Kamehameha)* would reestablish communications using proper R/T procedures.

EMERGENCY SILENCE

Emergency silence may be imposed on an R/T net only by competent authority. If an authentication system is in effect, a station must always authenticate a transmission that:

- Imposes emergency silence;
- Lifts emergency silence; and
- Calls stations during periods of emergency silence. When emergency silence is imposed, no receipt or answer for such transmissions is required.

To impose emergency silence, the NECOS speaks the proword SILENCE three times. For example, refer to figure 2-1 and assume that *Key* (net control) was authorized to impose emergency silence. *Key* would transmit:

"Poseidon, THIS IS Key, SILENCE, SILENCE, SILENCE, TIME One Four Four Zero Zulu, OUT."

To impose emergency silence on a particular frequency but not on all frequencies used in the net, *Key* would use the proword SILENCE (spoken three times), followed by a frequency or the frequency designator to be silenced. SILENCE (spoken three times), followed by the words "all nets,"means to cease transmissions immediately on all nets. All transmissions end with the proword OUT.

To lift emergency silence, *Key* would send the following transmission:

"Poseidon, THIS IS Key, SILENCE LIFTED, TIME One Five One Zero Zulu, OUT."

EXECUTIVE METHOD FOR RADIOTELEPHONE

The Executive Method for R/T is used to execute a tactical message at a given instant. This method is used to ensure that two or more units make simultaneous maneuvers. Abbreviated plaindress format is normally used for Executive Method messages. These messages never have a time group included in the message ending. There are two variations of the Executive Method: delayed and immediate.

DELAYED EXECUTIVE METHOD

A tactical message sent by the Delayed Executive Method must carry the warning proword EXECUTIVE TO FOLLOW in the message instructions immediately preceding the text. The executive signal is sent later in the form of "standby—EXECUTE," the latter word being the instant of execution. For example, referring to

figure 2-1, assume that *Key* sends the following message by the Delayed Executive Method to the collective call Poseidon:

"Poseidon, THIS IS Key, EXECUTE TO FOLLOW, Fire One Water Slug, OVER."

All stations respond in alphabetical order of full call signs:

"THIS IS Kamehameha, ROGER, OUT."

"THIS IS Polk, ROGER, OUT."

"THIS IS Tecumseh, ROGER, OUT."

"THIS IS Vallejo, ROGER, OUT."

When ready to execute, *Key* transmits:

"Poseidon, THIS IS Key, Standby, EXECUTE, OVER."

The stations then respond in alphabetical order of full call signs with:

"THIS IS (station), ROGER, OUT."

If communications conditions are good, *Key* can designate only one station to receipt for everyone to ensure that the transmission is heard. As part of the execute signal, *Key* could have transmitted:

"Poseidon, THIS IS Key, Standby, EXECUTE, Polk, OVER."

Polk would then ROGER with:

"THIS IS Polk, ROGER, OUT."

When considerable time has elapsed between the EXECUTE TO FOLLOW message and the actual execution message, the text to be executed should be repeated prior to the words "Standby—EXECUTE." The text should also be repeated when it is only a portion of a message or one of several outstanding "EXECUTE TO FOLLOW" messages.

IMMEDIATE EXECUTIVE METHOD

In cases of urgency, the execute signal may be transmitted in the final instructions element of the message to which it refers. The use of the Immediate Executive Method does not allow stations to obtain verifications, repetitions, acknowledgments, or cancellations before the message is executed. These messages should be in plain language or limited to basic TURN, CORPEN, and SPEED signals.

The Immediate Executive Method uses the warning proword IMMEDIATE EXECUTE in the message instructions instead of the proword EXECUTE TO FOLLOW. The text of the signal is transmitted twice, separated by the proword I SAY AGAIN. The execute signal is transmitted in the final instructions. For example:

"Poseidon, THIS IS Key, IMMEDIATE EXECUTIVE, BREAK, Shift Your Rudder, I SAY AGAIN, Shift Your Rudder, STANDBY, EXECUTE, Polk, Vallejo, OVER."

Notice that *Key* includes both *Polk* and *Vallejo* as ROGER addressees. Again, this is done to ensure that the transmission is received by everyone involved, provided communications are good. However, if communications are bad, all stations in the net must ROGER the execution. Upon hearing their calls, *Polk* and *Vallejo* would answer:

"Key, THIS IS Polk, ROGER, OUT"

"Key, THIS IS Vallejo, ROGER, OUT."

RADIOTELEPHONE CIRCUIT LOGS

R/T circuit logs must be maintained on all R/T nets or circuits unless otherwise directed. The circuit log shows a complete and continuous record of all transmitted and received traffic, as well as the operating condition on that radio day. Circuit logs contain the following information:

- Times of opening and closing by individual stations;
- Causes of any delays on the circuit;
- Frequency adjustments and changes;
- Unusual occurrences, such as procedural and security violations; and
- Changing of the watch.

NTP 5 contains the complete list of data required in an R/T circuit log.

When operating conditions permit and when there are no instructions to the contrary, an operator should record every transmission heard, regardless of the source or completeness. This rule applies to all tactical, command, and reporting nets. On other nets, a modified log may be kept.

Some nets may require only a modified log for ready reference. However, on nets or circuits that require complete logs, automatic recording devices

should be used to ensure a total record. Time should be automatically or manually recorded at intervals not to exceed 5 minutes.

When a message is addressed to or is to be relayed by the receiving station, the message must be written in full on a message blank. Only details needed to identify the message are inserted in the radio log. If the message does not need to be recorded in full on a message blank, the transmission should be recorded as completely as feasible in the circuit log.

When opening a new circuit or starting a log for a new day, the operator writes or types in his or her name and rank/rate or grade in full. Upon being relieved or closing the circuit, the operator must sign the log. The oncoming operator then writes or types his or her name and rank/rate or grade in full in the log.

Log entries are **never** erased. Any necessary changes are made by drawing a neat single line through the original entry and indicating the changed version adjacent to the lined out entry. When using the typewriter, the operator may use the slant key to delete erroneous entries. All changes must be initialed by the operator making the change.

SUMMARY

Circuit discipline is achieved through the proper use of radio equipment, adherence to prescribed frequencies and operating procedures, proper training, and monitoring. The lack of circuit discipline, as well as basic negligence, inaccuracy, and laxity, is responsible for violations that endanger the integrity and security of R/T transmissions.

It is essential that operators be well trained in proper communications voice procedures to competently perform their duties. They are responsible for maintaining circuit discipline at all times. Reliability, security, and speed of communications are reduced when operators don’t follow prescribed procedures.

CHAPTER 3

EMISSION CONTROL

Upon completing this chapter, you should be able to do the following

- *Identify EMCON and the procedures, including criteria, objectives, notification, and authority to set EMCON conditions both at sea and ashore.*
- *Identify the procedures, including criteria and actuation of HERO conditions.*
- *Identify alternate methods of communication during HERO and EMCON conditions, including electronic systems UHF AUTOCAT, SATCAT, and MIDDLEMAN and non-electronic relay systems PIGEON POST and BEAN BAG.*

Emission control (EMCON) is the management of electromagnetic and acoustic emissions. EMCON is used to prevent an enemy from detecting, identifying, and locating friendly forces. It is also used to minimize electromagnetic interference among friendly systems. EMCON is normally imposed by the electronic warfare coordinator (EWC) to control all electromagnetic radiations. Once EMCON is imposed, general or specific restrictions may be added to the EMCON order, depending on the operational, intelligence, or technical factors for the area affected.

For radiomen, EMCON usually means either full radio silence or HF EMCON. The most secure communications methods during EMCON reduce, but do not eliminate, the possibility of identification. It is assumed that any electromagnetic radiation will be immediately detected and the position of the transmitting ship will be fixed by an enemy. You will find detailed information on the implementation of EMCON and its degree of adjustment in *Fleet Communications,* NTP 4, and *Electronic Warfare Coordination,* NWP 10140 (NWP 3-51.1).

SETTING EMCON CONDITIONS

Setting EMCON requires four basic steps: criteria, objectives, notification, and authority. Details of these steps are found in the above listed publications. Basic requirements are listed below.

CRITERIA

To react to EMCON changes, each ship will prepare an EMCON bill that provides for implementing the EMCON condition in effect by:

- Outlining planning considerations for establishing the appropriate shipboard emitter status
- Assigning specific duties and responsibilities to personnel who control electromagnetic or acoustic emitters
- Establishing an EMCON control center with overall responsibility for shipboard emitter radiation status
- Designating intermediate control stations as required through which specific equipment is controlled
- Designating individual responsibility for each shipboard emitter
- Providing procedures for intraship reporting, verification (check off) of emitter status, and monitoring of own ship's emitter status.

OBJECTIVES

The objectives of EMCON are to deny the enemy any way that it may locate your position, to support the

efforts to disrupt the enemy's electiveness, and to allow your actions to go unnoticed. To accomplish these objectives, EMCON conditions are designed with the following guidelines:

- Minimize detection by enemy sensors
- Allow effective friendly command and control (C2)
- Support operations security (OPSEC)
- Support operational deception (OPDEC)
- Minimize interference among friendly systems
- Degrade effectiveness of enemy C2

NOTIFICATION

All ships need to keep command and control informed of any actions that may restrict, change, or alter in any way communication functions. The most fundamental of these actions follow:

- If at all possible, ships should notify the shore station of scheduled periods of EMCON due to radiation restrictions (HERO, HERF, RADHAZ) or other events (man aloft, aircraft operations, etc.) prior to the actual restrictive period.
- If EMCON is imposed without notice, relay procedures to deliver outgoing traffic may be attempted. Shore stations must be alert to the sudden, unscheduled imposition of EMCON and the accompanying lack of any transmission from the ship.
- Guidance for each EMCON condition must be posted at each station or space with responsibility for setting or monitoring a given EMCON condition for the emitters.
- If the ship should enter EMCON without prior notice, the shore station will keep a listening monitor on the ship's frequencies until the ship returns to the air. Additionally, a listening watch will be kept on the HICOM (covered and uncovered) net for possible contact from the ship.
- Once a ship with a multichannel (VFCT) termination has returned to the air on previously assigned frequencies, the orderwire will be restored before the traffic circuits. If the ship maintains a single channel (FSK) termination, the circuit will be reestablished via the technical control center.

AUTHORITY TO IMPOSE EMCON

EMCON is imposed as directed by the task group, squadron, or local instructions and standard operations procedures.

HAZARDS OF ELECTROMAGNETIC RADIATION TO ORDNANCE (HERO)

A danger of RF radiation is the risk of premature firing of ordnance or explosion of their warheads during loading and offloading operations. The hazard to electronic explosive devices (EEDs) occurs because of the heat generated by a current passing through the sensitive wires surrounding a temperature-sensitive explosive. If energy is dissipated into the wires, current will flow, the explosive will become hot, and an explosion can result.

CRITERIA

When ordnance or their warheads are loaded, unloaded, or transferred, shipboard HERO conditions may sometimes prohibit the transmission of RF frequency energy below 30 MHz. To maintain communication when HERO conditions are in effect, you will be required to use other frequencies or communication methods.

ACTUATION

Transmitters and their antennas have only one purpose, which is to radiate electromagnetic energy. The initiating elements of ordnance items need only to be supplied with the proper amount of energy for an explosion to take place. RF energy may enter a weapon through a hole or crack in the skin of the weapon. RF energy may also be conducted into the weapon by the firing leads or other wires that penetrate the weapon enclosure.

The probability of unintentional EED actuation is not totally predictable since detonation depends upon such variables as frequency, field strength, and environment. In general, ordnance systems that have proven to be susceptible to RF energy are most susceptible during loading, unloading, and handling in RF electromagnetic fields.

ALTERNATE METHODS

There will be times when you are unsure of the exact frequency of the active ordnance. In these circumstances you will be required to use alternate methods for communications. The alternate methods of relaying communications during HERO conditions include both electrical and nonelectrical relay systems.

Electrical

To provide an uninterrupted flow of essential communications without violating HERO and EMCON limitations, techniques called AUTOCAT, SATCAT, and MIDDLEMAN were developed. These techniques extend the range of relay procedures using amplitude modulation UHF transmission via HF or satellite. In AUTOCAT, a ship provides the method for automatically relaying UHF transmissions; in SATCAT, an airborne platform provides the method. In MIDDLEMAN, the objective is obtained; however, the method requires an operator to copy the message with subsequent manual retransmission.

AUTOCAT, SATCAT and MIDDLEMAN use three different types of circuit configurations for reception and relay of UHF transmissions. These circuits are:

- A voice circuit where some units send and receive on one frequency, and other units send and receive on any other frequency;
- A voice circuit where all units transmit on one frequency and receive on another frequency;
- A RATT circuit where all units transmit on one frequency and receive on another frequency.

Non-Electronic Relay Systems

There are two additional message relay systems. These systems, which utilize non-electronic relay systems, are PIGEON POST and BEAN BAG.

- PIGEON POST provides a method of traffic delivery to shore by aircraft;
- BEAN BAG provides a method for small ships to deliver message traffic via helo to shore or to a unit that is terminated full period for further transmission.

SUMMARY

EMCON is one of those facets of security that is required to properly perform your duties within general security guidelines. You must perform your duties in such a manner as to protect the integrity and overall value of secure communications.

We have discussed a number of differing types of communications, but have not covered procedures in detail. Use of local instructions, Task Force/Group battle orders, or other methods of relaying communications is required.

CHAPTER 4

CRYPTOSECURITY

Upon completing this chapter, you should be able to do the following:

- *Identify the procedures, methods, and steps for the destruction of Secret and below material.*
- *Identify the procedures used for the verification of destruction records of Secret and below material.*
- *Identify the procedures for receipt, inspection, inventory, control, destruction, and verification of destruction of SPECAT or Top Secret and above material.*
- *Identify the procedures for receipt, inspection, inventory, control, destruction, and verification of destruction of COMSEC material.*
- *Identify the procedures used when submitting required CMS reports to the CMS custodian.*

In this chapter we will address both general classified material and COMSEC material that deals with cryptosecurity in broad terms. The COMSEC portion is written from the perspective of the local holder's, local holder alternate's, and user's responsibilities.

As a Radioman, you will be required to handle many different types of material. You must know the correct procedures for receiving, inventorying, destroying, and providing all required documentation for this material.

General classified material usually is considered classified messages, publications, and instructions. COMSEC material is material used to protect U.S. Government transmission, communications, and the processing of classified and sensitive unclassified information. This is related to national security protection from unauthorized persons and material allowing for the authenticity of all such communications.

The protection of vital and sensitive information moving over government communications systems is crucial to the effective conduct of the government and specifically to the planning and execution of military operations. For amplifying information on the handling of classified material, consult *Information and Personnel Security Program Regulations* (OPNAVINST 5510. 1). For COMSEC material, *refer to Communications Security Material System (CMS) Policy and Procedures Manual,* CMS 1.

SECRET AND BELOW MATERIAL DESTRUCTION

Classified material that is no longer required should not be allowed to accumulate. Superseded and obsolete classified materials that have served their purpose should be destroyed in accordance with CMS 1 and local requirements.

The following information is presented not with the intent to give complete instructions or requirements; but rather as an overview of basic methods.

METHODS OF DESTRUCTION

Routine destruction of Secret and below material may be accomplished by burning, pulping, pulverizing, or shredding. Every command has a locally produced destruction SOP; this SOP will detail the specific requirements for your duty station.

DESTRUCTION

Secret material will be destroyed following the two-person rule without a record of destruction. If only one person destroys Secret material, a record of destruction must be made.

When destroying Confidential material, personnel must have a clearance level equal to or greater than the material. No record of destruction is required.

The commanding officer may impose additional controls at his or her discretion.

COMPLETE DESTRUCTION REPORTS

Destruction reports will be made in accordance with OPNAVINST 5510.1 and local instructions.

VERIFY DESTRUCTION RECORDS

To verify destruction records, the senior person will ensure that the material has been completely destroyed and only residue remains. All blanks are filled in correctly on the destruction report (if one is required), and it is turned into the proper authority.

SPECAT OR TOP SECRET AND ABOVE MATERIALS

Classified material that is of a more sensitive nature requires more "eyes-on" and "paper-trail" procedures. These materials must be provided control and accounting that relates to their assigned classification. This will limit the dissemination, reproduction, and viewing by personnel who, in the course of their duties, require access.

RECEIVE

SPECAT or Top Secret will normally be handled at the E-6 and above level. If receipt of this material is a recurring event at the command, follow the guidelines in OPNAVINST 5510.1, and local instructions.

INSPECT

Upon receipt of SPECAT, TOP Secret, or above material, ensure that all receipts and material are identified and verified prior to acceptance of the material.

INVENTORY

Material will be logged in the Top Secret log and placed in the appropriate safe.

CONTROL

Access to SPECAT, Top Secret, or above material will be closely guarded on a need-to-know basis. All material must be accounted for by signature.

DESTROY

Top Secret material will be destroyed by two witnessing officials. Those performing the destruction must have a clearance level equal to or greater than the material being destroyed.

Destruction of SPECAT and Top Secret and above material was covered in depth in module 1.

VERIFY DESTRUCTION

For information and procedures relating to verifying the destruction of SPECAT and Top Secretor above material, refer to OPNAVINST 5510.1 and local instructions.

COMSEC MATERLAL

Communications security (COMSEC) is a framework that allows the NAVY a unique distribution system that takes into account strict accountability and control procedures. The requirements for this system are exacting to ensure proper use of the cryptosystems in all areas.

RECEIVE

To receive material into local custody is to accept the responsibility for the proper handling, safeguarding, accounting, and disposition of COMSEC material issued by the custodian and user personnel. Every person who receives COMSEC material must complete a CMS Responsibility Acknowledgement Form, which is located in Annex K of CMS 1. This signed form must be on file with the CMS Custodian.

INSPECT

Local holders (LHs) will inspect the material that is issued for their use. They should verify that all material listed on the SF-153 is physically accounted for, check that all short titles and accounting numbers match, and

have any questions for use or storage answered prior to acceptance of the material.

INVENTORY

LH custodians must main a local custody file containing effective signed local custody documents. These will list all material in their possession. A watch station must maintain a watch-to-watch inventory that lists all COMSEC material held. This material is to be listed by short title, edition, accounting numbers, and quantity.

CONTROL

Watch-to-watch inventory is used to maintain control of effective material and material to be used in the future. Effective and supersession dates for all COMSEC material (less equipment and related components and devices) that the watch holds must have clearly marked dates in accordance with Article 760 of CMS 1.

DESTROY

Destruction of superseded material must be accurately documented and conducted within the required time frame. Article 790 of CMS 1 contains destruction procedures, and chapter 5 delineates personnel, methods, and time periods for destroying COMSEC material.

VERIFY DESTRUCTION

Refer to CMS 1 and local instructions for procedures to verify destruction of all COMSEC materials.

REQUIRED CMS REPORTS SUBMITTED TO CMS CUSTODIAN

CMS reports to the CMS Custodian normally include destruction reports and SF-153's that contain material that is to be returned to the CMS Custodian.

Further information on reports that the CMS Custodian may require are found in detail in CMS 1 and its various annexes.

SUMMARY

Security precautions will protect the integrity of the systems that are in place as long as you, as the radioman, understand and carry out the correct methods for handling, inventorying and destruction of required classified or COMSEC material. Security considerations presented in this chapter will not guarantee protection, nor do that try to cover all required areas. You will have to research and familiarize yourself with all requirements at the command or area that you are working in.

APPENDIX I

GLOSSARY

A

AUTHENTICATION— A security measure designed to protect a communications or command system against fraudulent transmissions or simulation.

AUTOMATIC DIGITAL NETWORK (AUTODIN)— A worldwide automatic communications system that provides automatic data service.

B

BEADWINDOW— A term describing a real-time procedure used to alert circuit operators that an unauthorized disclosure has occurred.

C

CARRIER— the unmodulated signal originally produced in the oscillator section of a transmitter.

CONFIDENTIAL— Information the unauthorized disclosure of which could reasonably be expected to cause damage to the national security.

CRYPTOSYSTEM— Information encompassing all the associated items of cryptomaterial that are used together to provide a single means of encryption or decryption.

D

DEFENSE SWITCHED NETWORK (DSN)— A nonsecure telecommunications telephone interconnected network among military and other government installations (formerly AUTOVON).

DIRECTED NET— A net in which member stations must obtain permission from the net control station (NECOS) prior to communicating with other stations on the net.

E

EMISSION CONTROL (EMCON)— General or specific restrictions placed on electromagnetic radiations for a particular area or areas.

F

FREE NET— A communications net of which member stations need not obtain permission of the net control station (NECOS) to transmit.

G

GATEGUARD— A security subsystem that allows commands to interface directly with the AUTODIN system as part of the NSTA program.

L

LOCAL HOLDER— A command or activity whose COMSEC material needs are met by drawing the material from a single CMS account.

M

MANUAL RELAY CENTER MODERNIZATION PROGRAM (MARCEMP)— An automation support system for all aspects of HF message relay operation in the Fleet Center.

P

PROSIGNS— Letters, or combinations of letters, that convey frequently sent orders or instructions in a simple, standard format.

PROWORDS— The phonetic equivalent of prosigns.

S

SECRET— Information the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security.

SECURE TELEPHONE UNIT THIRD GENERATION (STU-III)— Desktop phone unit that provides users with both clear and secure voice and data transmissions.

SEED KEY— Special keying material used for the initial electronic set-up of the STU-III terminal.

SERVICE MESSAGE— A short, concise message between communication personnel requiring prompt attention.

APPENDIX II

GLOSSARY OF ACRONYMS AND ABBREVIATIONS

A

AGT— AUTODIN Gateway Terminal

AIG— Address indicating groups

AIS— Automated Information System

AIT— AUTODIN Interface Terminal

ASC— AUTODIN Switching Center

AST— AUTODIN Subscriber Terminal

AUTODIN— Automatic Digital Network

AUTOVON— Automatic Voice Network

B

BIU— BUS interface unit

C

C2— Command and control

CAI— Communication Action Identifier

CDPS— Communication Data Processing System

CIC— Combat Information Center; Content Indicator Code

CIK— Crypto-ignition key

CIN— Component identification number

CMS— Communications Security Material System

COMSEC— Communications security

COMNAVCOMTELCOM— Commander, Naval Computer and Telecommunications Command

CUDIXS— Common User Digital Information Exchange System

CSN— Channel service number

D

DCS— Defense Communications System

DSN— Defense Switched Network

E

EDPE— Electronic data processing equipments

EEFI— Essential Elements of Friendly Information

EMCON— Emission control

EOM— End of message

EWC— Electronic warfare coordinator

F

FIFO— First-in-first-out

FLTSATCOM— Fleet Satellite Communications

G

GD— Guard device

GMT— Greenwich mean time

H

HARPS— Hybrid AUTODIN Red Patch Service

HERO— Hazards of Electromagnetic Radiation to Ordnance

I

I/O— Input and output

K

KMC— Key Management Center

L

LDMX— Local Digital Message Exchange

LH— Local Holder

M

MAN— Message accountability number

MARCEMP— Manual Relay Center Modernization Program

MLPP— Multilevel precedence and preemption

MSL— Master Station Log

MS/DOS— Microsoft® Disk Operating System

MTTS— Magnetic tape terminal station

N

NAVCOMPARS— Naval Communications Processing and Routing System

NAVMACS— Naval Modular Automated Communications System

NCS— Net Control Station

NECOS— Net Control Station

NST— Navy Standard Teleprinter

NSTA— Navy Standard Teleprinter Ashore

NTC— Naval Telecommunications Center

O

OAS— Office automation system

OPDEC— Operational deception

OPSEC— Operational security

OTAR— Over-the-air Rekey

OTAT— Over-the-air Transfer

P

PCMT— Personal Computer Message Terminal

PLA— Plain language address

R

RAM— Random-access memory

RI— Routing indicator

RIXT— Remote Information Exchange Terminals

R/T— Radiotelephone

S

SID— Subscriber identification

SOPA— Senior officer present afloat

SSIXS— Submarine Satellite Information Exchange Subsystem

SSN— Station serial number

STU-III— Secure Telephone Unit Third Generation

SUSDUPE— Suspected duplicate

T

TCC— Telecommunications Center

V

(V)— Version (e.g., (V)5...fifth version)

VDT— Video display terminal

W

WWMCCS— Worldwide Military Command and Control System

APPENDIX III

REFERENCES USED TO DEVELOP THE TRAMAN

Automatic Digital Network (AUTODIN) Operating Procedures, JANAP 128(J), Joint Chiefs of Staff, Washington, D.C., July 1993.

Basic Operational Communications Doctrine (U), NWP4(B) (NWP 6-01), Chief of Naval Operations, Washington, D.C., September 1989.

Call Sign Book for Ships, ACP 113(AC), Joint Chiefs of Staff, Washington, D.C., April 1986.

Communication Instructions—General (U), ACP 121(F), Joint Chiefs of Staff, Washington, D.C., April 1983.

Communications Instructions—Security (U), ACP 122, Joint Chiefs of Staff, Washington, D.C., 1981.

Communications Instructions—Tape Relay Procedures, ACP 127(G), Joint Chiefs of Staff, Washington, D.C., November 1988.

Communications Instructions—Tape Relay Procedures, ACP 127 US SUPP-1(H), Joint Chiefs of Staff, Washington, D.C., May 1984.

Communications Instructions—Teletypewriter (Teleprinter) Procedures, ACP 126(C), Joint Chiefs of Staff, Washington, D.C., May 1989.

Communications Security Material System (CMS) Policy and Procedures Manual, CMS 1, Department of the Navy, Washington, D.C., March 1993.

Department of the Navy Information and Personnel Security Program Regulation, OPNAVINST 5510.1H, Chief of Naval Operations, Washington, D.C., May 1991

Fleet Communications (U), NTP 4(C), Commander, Naval Telecommunications Command, Washington, D.C., June 1988.

Joint Voice Call Sign Book, JANAP 119, Joint Chiefs of Staff, Washington, D.C., January 1984.

Radiotelephone Procedure, ACP 125(E), Joint Chiefs of Staff, Washington, D.C., August 1987.

Secure Telephone Unit Third Generation (STU-III) Comsec Material Management Manual (CMS6), Communications Security Material System, Washington, D.C., October 1990.

Telecommunications Users Manual, NTP 3(I), Commander, Naval Telecommunications Command, Washington, D.C., January 1990.

Voice Communications, NTP 5(B), Naval Telecommunications Command, Washington, D.C., August 1984.

INDEX

Assignment Questions

Information: The text pages that you are to study are provided at the beginning of the assignment questions.

ASSIGNMENT 1

Textbook Assignment: “Center Operations,” chapter 1, pages 1-1 through 1-23.

1-1. The PCMT system is the central part of what larger Navy communications system?

1. NSTA
2. MARCEMP
3. IMARSAT
4. DSN

1-2. What does the PCMT software package combine for message-processing?

1. BIUs and IBM-compatible PC desktop microcomputers
2. PC-compatible desktop microcomputers
3. Desktop microcomputers and mainframe computers
4. Mainframe computers and HAVC super computers

1-3. What type of message-processing system is the PCMT system?

1. Basic
2. dBase
3. Store-and-forward
4. Network

1-4. What is the minimum amount of RAM for the PCMT microprocessor to have?

1. 1GB
2. 2GB
3. 760K
4. 640K

1-5. When trying to recall a message from the hard disk on the PCMT system, you can recall it by its MAN, CIN, or what other factor?

1. DTG
2. TOR
3. CSN
4. TOT

1-6. The PCMT outputs its message traffic for the user to what device?

1. Hard drive
2. Diskette
3. CD - ROM
4. CD

1-7. Which of the following systems replaced NAVCOMPARS?

1. NSTA
2. DSN
3. INMARSAT
4. MARCEMP

1-8. What is the maximum number of send and receive channels that can be handled simultaneously using MARCEMP?

1. 12 send/24 receive
2. 24 send/12 send
3. 12 send/12 receive
4. 24 send/24 receive

1-9. Approximately what maximum number of narrative or operator-to-operator messages are processed daily on MARCEMP?

1. 1,500
2. 2,800
3. 3,500
4. 4,000

1-10. What does the GateGuard subsystem provide for the user?

1. A path to AUTODIN
2. A secure access to the Internet
3. A means to send message traffic to the communications center
4. A user friendly terminal in which to communicate with the computer

1-11. What are the three elements of the GateGuard System?

1. AIT, OAS, and TCC
2. AGT, GD, and AIT
3. AGT, AIS, and GD
4. TCC, OAS, and GD

1-12. Besides serving as a gateway to AUTODIN, GateGuard has which of the following functions?

1. Speeds processing time
2. Removes interference from the communications center
3. Allows use of all networks
4. Serves as security guard device

1-13. What is the path using GateGuard from the AST to the GD?

1. AST, AGT, then to GD
2. AGT, ASR, then to the firewall
3. AST to GD
4. AGT, AST, then to GD

1-14. What does the AST provide to the AGT?

1. Long-term storage
2. Long-term archive storage
3. Temporary storage
4. Store and forward

1-15. Who manages the AUTODIN system?

1. NSA
2. CNCTC
3. DCA
4. DCS

1-16. What is the “backbone” of the AUTODIN system?

1. TCC
2. RCS
3. DCA
4. ASC

1-17. What is the total number of AUTODIN operational modes?

1. 7
2. 6
3. 5
4. 4

1-18. Which mode is used with unidirectional operation only?

1. I
2. II
3. III
4. IV

1-19. What are two types of I/O coded languages?

1. ASCII and Hollerith
2. ASCII and ITA #2
3. ITA #2 and Hollerith
4. Five level tape and card punch

1-20. Routing indicators have what minimum number of letters?

1. Seven
2. Six
3. Five
4. Four

1-21. In a routing indicator what does the third letter identify?

1. International alliance
2. Geographical area
3. Designate relay
4. Tributary station

1-22. During transmission of a message, what is the symbol ZCZC used for?

1. Signifies the start of the message
2. Starts the routing indicator series
3. The station designator
4. Geographical area for the final processing station

1-23. What precedence of message traffic will (a) preempt all other traffic, and (b) what is its position in the message header?

1. (a) Yankee (b) 1
2. (a) Yankee (b) 3
3. (a) Immediate (b) 1
4. (a) ECP (b) 2

1-24. In the classification position of a message, the letter “A” represents what classification or special handling instruction?

1. Top Secret
2. Secret
3. SPECAT
4. Confidential

1-25. In positions 5 through 8, a CAI of ZYVW tells the operator that this is what type of message?

1. EAM
2. Service
3. Information
4. Pass-through

1-26. At a tributary station the TOF and TAD are used for what reason?

1. Determine message-processing times
2. Calculate delivery times only
3. Calculate delivery and source times
4. Determine message receipt times

1-27. What types of messages of up to 100 lines can be sent without paging the text?

1. NAVAIR and NOTAMs
2. HYDROLANT and HYDROPAC
3. Statistical and meteorological
4. Data image and tributary

1-28. When a message may have been transmitted before, but you are not sure, you should forward the message with what marking in the header?

1. RETRANS
2. SUSDUPE
3. EDPE
4. MTTS

1-29. When, if ever, will a station usually notice that a message has been missent to the command?

1. Upon its arrival at the command
2. At the ASC switch
3. At the TCC
4. Never

1-30. How do you as an operator identify a misrouted message?

1. It has one or more incorrect PLAs
2. It has no routing instructions
3. It has no security coding
4. It contains incorrect routing instructions

1-31. In which of the following types of tapes are you NOT permitted to have splices?

1. History
2. Backup
3. Data pattern
4. Traffic

1-32. If a message has mismatched security classifications in a single-address message, what action will the ASC take?

1. Drop to the service clerk at the ASC
2. Correct the mismatch
3. Reject the message back to the originator only
4. Reject the message and alert the originating terminal

1-33. What version is considered the most sophisticated of all the NAVMACS systems?

1. V1
2. V1-MPD
3. V3
4. (V)5/(V)5A

1-34. For Navy use, NAVMACS is based on which of the following factors?

1. Security
2. Needs of the individual ships or commands
3. Fleet communications area wide requirements
4. Software and hardware considerations

1-35. In the system designated NAVMACS (V)2-MPD, what does MPD stand for?

1. Modified video displays
2. Military visual deployments
3. Multi-facet variable displays
4. Multi-functional digital download

1-36. Which of the NAVMACS systems has up to four channels of full-period termination send-and-receive circuits?

1. (V) 1
2. (V) 2
3. (V) 3
4. (V)5/(V)5A

1-37. What system in the fleet communication systems utilizes SID numbers?

1. NAVMACS
2. CDPS
3. SSIXS
4. CUDIXS

1-38. Of the many fleet communication systems, which one provides an optional satellite path to complement existing VLF/LF/HF broadcasts?

1. CUDIXS
2. CDPS
3. NAVMACS
4. SSIXS

1-39. What is the net cycle range on a CUDIXS/Subscriber Net Cycle?

1. 10 to 120 sec
2. 20 to 120 sec
3. 25 to 120 sec
4. 30 to 120 sec

1-40. What class of ships utilizes the CDPS?

1. DDG
2. LHA
3. FFG
4. FF

1-41. When a submarine uses SSIXS, what (a) position must be maintained to transmit/receive to/from the satellite and (b) in what tactical situation?

1. (a) Over-the-horizon
   (b) deep running
2. (a) Line-of-sight
   (b) mast-mounted antenna exposed
3. (a) Surface-to-air
   (b) submerged
4. (a) Ship-to-shore
   (b) long wire extended

1-42. What system is used between submarines and submarines and shore stations?

1. CDPS
2. CUDIXS
3. NAVMACS
4. SSIXS

1-43. What organization has certified the use of STU-III equipment up to Top Secret?

1. COMNAVCOMTELCOM
2. SPAWAR
3. CIA
4. NSA

1-44. How is secure mode in the STU-III unit activated and deactivated?

1. Turning the key to the local position to place the call and then to the remote once the called party has answered
2. Activated by the user key and deactivated by its removal
3. Using a CIK
4. By unplugging and re-plugging the STU-III

1-45. To obtain information on the management of STU-III terminals, you should use what publication?

1. CMS 6
2. CMS 1
3. CMS 5
4. CMS 3B

1-46. Precedence and preemption used in DSN are known by which of the following terms?

1. MLPP
2. PREEMPT
3. PREC
4. OVERRIDE

1-47. What is the total number of call treatments on the DSN system?

1. One
2. Five
3. Six
4. Four

1-48. Of the call treatments, which one is preempted only by FO?

1. F
2. I
3. P
4. R

1-49. Of the following systems, which is NOT secure?

1. CDPS
2. CUDIX
3. DSN
4. STU-III

1-50. As an operator you have received an immediate contact report which does NOT have the proper authentication. What should you do with this report?

1. Try to reverify the message
2. Place the message in the hold box for the supervisor
3. Relay or retransmit the message
4. Disregard the message

1-51. Which of the following methods is used to protect a system against fraudulent transmissions?

1. Semaphore
2. Authentication
3. Nancy system
4. Ship-to-shore

1-52. Who is responsible for preparing the command guard list?

1. Each command
2. The TYCOM
3. Each area commander
4. The FLTCINCs

1-53. For what minimum period is the MSL retained?

1. 30 days
2. 90 days
3. 6 months
4. 12 months

1-54. What are the two type of keys used with the STU-III?

1. CIK and blank
2. CIK and seed
3. Seed and ignition
4. Seed and master

1-55. How many different manufacturers of the STU-III are there?

1. One
2. Two
3. Three
4. Four

1-56. When using the STU-III terminal,what modes of operation are open to your use?

1. Fax and burst transmission
2. Clear voice and clear data
3. Secure voice and secure data
4. Both 2 and 3 above

1-57. Where in the CIK is the information contained to seed the STU-III terminal?

1. In the microchips
2. In the expandable memory
3. In the ignition points
4. In the metal strip

1-58. In what publication will you find R/T procedures for reporting enemy contacts?

1. ACP 125
2. ACP 135
3. NTP 3
4. NTP 4

1-59. In what publication will you find enemy contact report instructions and procedures?

1. ACP 124
2. ACP 125
3. ATP 3, VOL I
4. ATP 1, VOL I

1-60. What does the communications plan do for your command?

1. Satisfies the communications requirements for an operation
2. Outlines the changing factors from ocean area to ocean area
3. Gives the exact number of personnel who will be required to operate the various systems during the event
4. Outlines the whole communications picture for each system

1-61. What is the nomenclature of the monitoring and evaluating system used by afloat forces?

1. AN/SYS-80
2. URC/143/T-1
3. AN/SSQ-88/A/B
4. QC-SYS-84

1-62. At what time does RADAY start worldwide?

1. 2359Z
2. 0000Z
3. 0001Z
4. 0002Z

ASSIGNMENT 2

Textbook Assignment: "Voice Communications," chapter 2, pages 2-1 through 2-23; "Emission Control," chapter 3, pages 3-1 through 3-3; and "Cryptosecurity," chapter 4, pages 4-1 through 4-3.

2-1. What is the easiest and most convenient method of relaying traffic from ship to ship ship to shore, or shore to ship?

1. R/T
2. SECVOX
3. DSN
4. SNEAKER-NET

2-2. Which of the following is NOT a good circuit technique?

1. Pause a few seconds after each normal phrase and interrupt your carrier
2. Speak slowly
3. Group words in a natural manner
4. Hold the handset button in the push-to-talk position until ready to transmit

2-3. What are prowords used for?

1. To expedite message handling on circuits where radio-telephone procedures are used
2. To replace "Q" and "Z" signals
3. To replace the phonetic alphabet
4. To allow area commanders to use brevity codes to expedite all coded traffic

2-4. What proword is used to replace "addressees immediately following are exempted from the collective call?"

1. EXECUTE
2. EXEMPT
3. INFO
4. IMMEDIATE EXECUTE

2-5. What proword is the equivalent of ZOF?

1. SERVICE
2. SPEAK SLOWER
3. TIME
4. RELAY

2-6. In what publication will you find Communication Instructions, Operating Signals?

1. ACP 131
2. JANAP 126
3. ACP 135
4. JANAP 128

2-7. What is the real-time procedure that tells an operator on a nonsecure voice circuit that he or she has made an unauthorized disclosure?

1. RAINFORM
2. WARNING ONE
3. BEADWINDOW
4. SECURITY

2-8. EEFI 03 is transmitted over a nonsecure voice circuit to you as an operator. What type of information have you revealed?

1. Position
2. Operations
3. Capabilities
4. COMSEC

2-9. After being “BEADWINDOWED,” what is your only response?

1. RETRANSMITTING AGAIN IN SECURE FORMAT
2. ROGER, STANDING BY
3. RETRANSMITTING FOR CLARITY FOR USER
4. ROGER, OUT

2-10. Where is the EEFI list posted?

1. Inside VOXCOM area
2. In clear sight at all nonsecure voice positions
3. On the back of the nonsecure phone
4. In the standing orders of the day

2-11. On a large ship where will you find most of the voice circuits that a commanding officer needs?

1. CIC
2. Radio
3. Radio two
4. Captain’s cabin

2-12. What publication lists the publications that contain encrypted and daily changing call signs?

1. ACP 110
2. ACP 113
3. NTP 5
4. NTP 4

2-13. Circuits that are used in port and are neither tactical nor operational are categorized as what type?

1. TACTCKT
2. Port operations
3. Tug control
4. Administrative

2-14. Who establishes the circuit requirements from port to port?

1. SOPA
2. Port Captain
3. Tug Control
4. Senior Pilot

2-15. What are the types of nets?

1. Free and control
2. Control and directed
3. Directed and free
4. Control, directed, and NECOS

2-16. What is NECOS’s function?

1. Responsible for operational procedures, discipline, and security
2. Shares a common circuit for security advisement
3. Collectively monitors all circuits for security
4. Directs the net in a civilian uprising or natural disaster

2-17. What is the difference between (a) a free net and (b) a directed net?

1. (a) You can use the net without permission
   (b) you must get permission from NECOS
2. (a) You can use either secure or nonsecure circuits
   (b) you must use only the secure net
3. (a) You can only use nonsecure circuits
   (b) you are free to use either secure or nonsecure circuits
4. (a) You can only call up those ships or commands on an administrative net
   (b) the NECOS will tell you whom you may call up

2-18. Who is responsible for opening or reopening a net?

1. CIC
2. NECOS
3. Communications Area Master Station
4. The last ship using the net

2-19. When a ship needs to pass traffic to another ship, how long in duration should the test signal be to tune the receiver or transmitter?

1. 10 sec
2. 20 sec
3. 25 sec
4. 30 sec

2-20. What is the correct method of receipting for a R/T message?

1. Pass in the blind the numbers being receipting for
2. Send a formatted class A type of message
3. Use the proword ROGER
4. Get on the secure voice and pass back the receipted message

2-21. You are the only ship when you receive a delayed executive method message. What is the correct method to respond?

1. THIS IS (STATION), ROGER, OUT
2. THIS IS (STATION). OUT
3. (STATION), ROGER, OUT
4. (STATION), OUT

2-22. You have received an “EXECUTE TO FOLLOW” command and several minutes have elapsed. What will be the correct EXECUTE command to initiate action?

1. EXECUTE
2. Standby, EXECUTE
3. EXECUTE, EXECUTE
4. EXECUTE TO FOLLOW, EXECUTE

2-23. In what publication will you find a complete list of the required information to be found on a R/T log?

1. NWP 0 (NWP 1-01)
2. NTP 5
3. NTP 3
4. NTP 4

2-24. When, if ever, can you legally erase an entry in a log?

1. If an entry contains a misspelling
2. If an entry was not placed at the correct time and the operator must completely rewrite the log with the correct entry placed at the correct time
3. If an entry contains incorrect information
4. Never

2-25. What are the two actions an operator must take to correct a log entry?

1. Use the X key to typeover the incorrect information and use white out to correct the erroneous entry
2. Use the slant key to type the information to be deleted and initial the entry
3. Erase the entry and retype it in full
4. Retype the entry underneath and then strike out the erroneous material with the slash key

2-26. What does EMCON mean?

1. Emergency condition
2. Emission control
3. Enemy control
4. Emission condition

2-27. What is EMCON?

1. The system to facilitate how emergency conditions are handled
2. An area that is off-limits for broadcasting into enemy controlled spaces
3. An emission condition that limits power outputs
4. The management of electromagnetic and acoustic emissions

2-28. Who usually imposes EMCON?

1. EWC
2. CIC officer
3. Radio officer
4. Commanding officer

2-29. As an operator, why do you not want to transmit any type of communications during EMCON?

1. You can burn up a transformer
2. Radiation patterns will allow your position to be distorted
3. You can be detected, and your position will be known
4. High levels of RF energy will be present in the radio shack

2-30. In what publications will you find the necessary detailed requirements, procedures, and guidelines to help you with the implementation of EMCON?

1. NTP 3 and NWP 3 (NWP 1-02)
2. NTP 3 and NTP 4
3. NWP 10-1-40 (NWP 3-51.1) and NWP 4 (NWP 6-01)
4. NTP 4 and NWP 10-1-40 (NWP 3-51.1)

2-31. Which of the following steps should be taken on each ship concerning EMCON?

1. Provide a check-off of emitter status
2. Designate individuals responsible for each emitter
3. Establish an EMCON control center with overall responsibility
4. All of the above

2-32. Who is responsible for planning and establishing a shipboard emitter status?

1. The TYCOM
2. Each ship
3. The FLTCINCs
4. The EWCs

2-33. Which of the following is NOT an objective of EMCON?

1. Reduce the power output of the emitters aboard ship
2. Support OPSEC
3. Degrade the enemy's C2
4. Allow effective friendly C2

2-34. When, if ever, should a ship notify the shore station of impending EMCON requirements for radiation restrictions?

1. Only if required in writing by the TYCOM
2. Before the restrictive period
3. Only during "Spook Ops", and only if required by the mission statement
4. Never; this could lead to the enemy intercepting the message

2-35. When returning to the air after EMCON, a ship with a VFCT termination is required to establish what circuit first?

1. The multichannel broadcast
2. SAR monitoring
3. DAMA
4. The orderwire

2-36. What is the frequency range that is prohibited for use during HERO conditions?

1. 10-15 MHz
2. 20-25 MHz
3. Below 30 MHz
4. Above 35 MHz

2-37. Why is RF radiation considered a threat?

1. RF burns
2. Premature firing of ordnance or explosion
3. High radiation pattern emissions
4. An overcrowded frequency band

2-38. What is the main cause of EEDs exploding during HERO?

1. Heat
2. Cold
3. Reversal in polarity
4. Dropping

2-39. What is the purpose of transmitters and their antennas?

1. To relay voice intelligence transmissions
2. To direct high patterns
3. To utilize low patterns
4. To radiate electromagnetic energy

2-40. When are ordnance most susceptible to RF energy fields?

1. One hour prior to firing
2. When they are being armed
3. During loading, unloading and handling
4. During dry firing

2-41. What are the alternate methods to communicate during HERO or EMCON conditions and limitations?

1. Non-electrical and subsonic
2. Electrical and non-electrical
3. Electrical and ferrous
4. Non-electrical and distributed

2-42. What is the total number of alternate electrical communications methods developed for use during EMCON and HERO conditions?

1. One
2. Two
3. Three
4. Four

2-43. During AUTOCAT, what provides the means for relaying the transmissions?

1. A ship
2. An airplane, and the Nancy system
3. A ship, an operator, and an LF transmitter
4. A ship, a COD flight, and two copies of each message

2-44. What is the main difference in the three types of alternate electrical methods of communications?

1. Physical means of transportation
2. Circuit configurations
3. Electrical means of radiation
4. Equipment restraints

2-45. What are the two types of non-electrical relay systems now in use?

1. MIDDLEMAN and BEAN BAG
2. AUTOCAT and SATCAT
3. SATCAT AND PIGEON POST
4. PIGEON POST and BEAN BAG

2-46. What non-electrical relay method uses aircraft?

1. CARRIER PIGEON
2. COD FLIGHT
3. PIGEON POST
4. SMALL BOY

2-47. What non-electrical relay method utilizes helicopters?

1. BEAN BAG
2. TIGHT DOOR
3. OPEN HATCH
4. LOST RANGER

2-48. What is the type of material that is used to protect U.S. Government transmissions, communications, and processing of sensitive unclassified information?

1. TOP SECRET
2. SECRET
3. COMSEC
4. Classified

2-49. In what publication will you find detailed information on COMSEC material handling?

1. CMS 1
2. CMS 5
3. CMS 3
4. CMS 6

2-50. What instruction covers the handling of classified material?

1. OPNAVINST C5510
2. SECNAVINST 2515
3. SECNAVINST 5238.1
4. OPNAVINST 5510.1

2-51. Which of the following methods is NOT an authorized technique of destruction?

1. Pulverizing
2. Chipping
3. Shredding
4. Pulping

2-52. If only a single person destroys Secret material what records, if any, are required?

1. Disclosure
2. Destruction
3. Eradication
4. None

2-53. What type of record, if any, is required when destroying Confidential material?

1. Eradication
2. Destruction
3. Disclosure
4. None

2-54. Who ensures that the material that is being destroyed has been completely destroyed and only residue is left?

1. The senior person present
2. The CMS custodian
3. The communications officer
4. The executive officer

2-55. What is the required paygrade level for receipt of SPECAT, Top Secret or above material?

1. E-1 through E-9
2. E-5 and above
3. E-6 and above
4. E-7 and above

2-56. How do you account for who has physical control of SPECAT, Top Secret, or above material?

1. By signature
2. By identification card
3. Letter of appointment
4. All of the above

2-57. What type of form is required for you to handle and use COMSEC material?

1. Local User form
2. CMS Responsibility Acknowledgement form
3. Local Holder form
4. COMSEC Material Issue form

2-58. Where will you find the original form that allows you to handle and use COMSEC material?

1. CMS 5, Annex I
2. CMS 3B, Annex A
3. NAG 16, Annex FF
4. CMS 1, Annex K

2-59. Where is the form kept that allows you as a user to handle and receipt for COMSEC material?

1. With DCMS
2. With the Local User custodian
3. With the Local Holder custodian
4. With the CMS custodian

2-60. Each communication watch station, section, or crew has an inventory of all the COMSEC material that the watch holds. The material is listed by accounting numbers, edition, short title, and what other item?

1. Number of unopened key cards
2. Prior destroyed editions
3. Quantity
4. Number of superseded canisters

2-61. In what publication and article will you find how COMSEC material must be marked for effective and superseded dates?

1. CMS 1, Art. 760
2. CMS 1, Art. 100
3. CMS 5, Art. 122
4. CMS 6, Art. 002

2-62. Which of the following chapters of CMS 1 details the personnel, methods, and time periods for destroying COMSEC material?

1. One
2. Five
3. Seven
4. Eight

2-63. When you as the LH custodian are required to return unused material to the CMS custodian, you should use what form?

1. SF-100
2. SF-210
3. SF-153
4. Unutilized Material Delivery